COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 31 August / août 2015 T-PD(2015)02Mos

CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA

COMITÉ CONSULTATIF DE LA CONVENTION POUR LA PROTECTION DES PERSONNES A L'EGARD DU TRAITEMENT AUTOMATISÉ DES DONNÉES A CARACTÈRE PERSONNEL [STE n°108]

COMPILATION OF REPLIES ON MEDICAL TECHNOLOGIES AND DATA PROTECTION ISSUES

Recommendation (97)5 on medical data
Questionnaire on Medical Data

****

Directorate General Human Rights and Rule of Law /
Direction Générale Droits de l'homme et Etat de droit

INDEX / TABLE DES MATIERES

ALBANIA / ALBANIE - THE COMMISSIONER
FOR FREEDOM OF INFORMATION AND PERSONAL DATA PROTECTION (IDP)

QUESTIONNAIRE

The questionnaire should ideally be completed by data protection authorities, health policy authorities, professional or patient associations as well as healthcare providers: you are invited to share it as widely as possible.

Please send your replies to dataprotection@coe.int no later than 15 December 2014.

1. Mobile Health (mHealth) and Electronic Health Records (EHR)

1.1. Data Protection Issues:

This is perhaps the biggest topic sitting at the intersection of technology and data protection. Mobile health (mHealth) and Electronic Health Records (EHR) are increasingly used in healthcare systems and provisions – it is a trend that needs to be examined.

Related to the EHR, these records are more accurate, cost-effective (in terms of storage) than paper-based notes. The concept of patient controlled/accessed EHR has been implemented in varying degrees in different countries.

Furthermore, some non-medical record can still contain health information about users and it should be considered if such records ought to be treated in a similar way to EHR.

Also, should 'medical data' as defined in Recommendation N° (97) 5 on the protection of medical data cover physical tracking data, such as pedometers or fitness data and data that can lead to medical information about an individual ?

1.2. Questions: if EHR exist in your country, is your legal framework providing for a regulation of such records? If mHealth exists in your country, is your legal framework providing for a specific regulation? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	In our country there is no specific legislation for EHR. For that reason is covered by the law "On protection of personal data", no. 9887 dated 10.03.2008, amended , and Instruction no. 5 of 26 may 2010 "On fundamendal rules concerning protection of personal data in the health care system" and Instruction no23, date 20.11.2012 "On processing personal data in the health sector" .
Case-law:	Some of the findings, made by the Inspection Department, during the inspection were: - Lack of internal regulations regarding security measures for personal data; - Lack of consent of the data subject (patient) in written form and demonstrable way; - Lack of fulfillment of the obligation to inform data subjects about the ways of data processing and the rights they have; - In the contracts with third parties, in order to delegate the processing, should be determined some rules concerning the security and confidentiality of data,

	deadlines and means of processing, access rights and ways of destroying data; - Violation of the principle of adequacy of data and exceeding the purpose of processing; - Keeping personal data for an indefinite term; - Limitation of access to systems processing personal data; - Lack of privacy policies on websites of controllers. Commissioner Authority is expressed through Recommendations, Orders and in cases of serious repeated and intentional violations, has established administrative sanctions (fines).
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
EHR and Medical data:	What can be considered medical data in your country? Is it solely the data relating to a person's health (state, diagnosis, prognosis, medical treatment, etc.)? Is non-medical data that leads to medical information treated the same way as medical data (for instance in terms of confidentiality requirements)? Is the EHR solely constituted of data collected in a medical context or can the individual also himself or herself add information regarding his or her health?
	In terms of the law is presumed that the medical record is the information that relates to an individual's medical records. These data are part of the special category of data called "sensitive data". The law makes no distinction between medical data and data that lead to their identification. The individual is not able to add information about his health.
Sharing of data and Access:	Who is granted access to the EHR and how is the sharing of information (with other health care providers?) regulated? Where information is shared with pharmacists, is there a strict purpose limitation in place? How has the definition of the responsibility over the medical data been regulated?
	Pursuant to Instruction no. 23, dated 20.11 2012 " On processing personal data in the health sector" Health care professionals have an obligation to share the information with the consent of the patient in accordance with the purpose of the information collected. The request for a data transmission by the third party must be made in writing, and must indicate the health data that are subject to the request along with the purpose of the request. The requested data must be adequate and necessary for fulfilling the purpose of the request. In case the health care provider learns that the data requested are not proportionate to the goal of the transmission, it shall notify the Commissioner for Protection of Personal Data immediately. Also, the transmission of health data shall be recorded, along with the recipient, the data subject to the data transmission, the purpose and date of transmission. These records shall be kept for 5 years.

Data quality:	Are the principles of legitimacy, fairness and minimisation applied to medical data? How are records kept accurate? How long is the data kept for, is the specific storage period defined for the EHR?
	These principles are provided in the instruction no. 23, dated 20.11 2012 "Processing of personal data in the health sector". Also, there are provided time limits, for the maintenance of health data. Health records shall be retained for 30 years from recording the last data included. Discard reports shall be kept for 50 years. Recordings made using imaging diagnostic methods shall be kept for 10 years. After the deadline, an assessment has to be made whether further retention is necessary for scientific purposes; otherwise, the data shall be deleted. If further retention is necessary for scientific purposes, the records shall be transmitted to the competent state archive. Pharmacies shall keep recipes for 2 years; recipes for narcotic or psychotropic materials shall be kept for 3 years and recipes for strong poisonous drugs shall be kept for 5 years. During the retention period, the readability and integrity of health records shall be maintained using technical measures. Rectification of false or misspelled data shall be carried out in a way that the original data are not cancelled even after rectification.
Data integrity:	Are any specific methods used to ensure the integrity of the data? How are patients identified in the EHR? In the context of research, are anonymisation methods used and what safeguards exist for re-identification?
	Under the instruction no. 23, dated 20.11 2012 "Processing of personal data in the health sector", for the purposes of scientific research, the researcher may access health records with the permission of the director of the health service provider. The publication shall not include health data that can be linked to an identified or identifiable person, only anonymous data. During the research, the researcher shall not copy records in a way that the copy includes health data that are not anonymous. Names of researchers accessing the recordings shall be recorded, along with the reason and time of access. The access log shall be kept for 10 years, and then it shall be deleted. Also, for the purposes of development of training materials used for demonstration in medical training and research, images, video recordings or sound recordings can be used upon the condition that they are anonymized.
Data security:	Where are the records stored? Is there a centralised database of EHR? What security technology is being used?
	Office of the Commissioner has approved the Instruction No. 21, date24/09/2012 On “Determining the rules for safeguarding the personal data processed by Large Controllers” which defines specific security rules for personal data protection processed manually or electronically.
Rights of the person/patient concerned:	How can the right of access be exercised? How can the data be corrected? Can the person enter information in his or her own EHR? What are the legal remedies available?
	Patient's rights are covered by Article 12 and 13 of Law No. 9887, dated 10.03.2008 "On protection of personal data", as amended, which is published in English version in the official website of the authority, www.kmdp.al

	Within 30 days from receipt of the data subject request, the controller must respond. Otherwise, the data subject has the right to appeal to the Office of the Commissioner.Following this complaint, in accordance with the Code of Civil Procedure, the data subject may file a complaint in court.
Consent:	Is the system based on an opt-in approach? Is the principle of granular consent applied (with the possibility of preventing access to certain data?)? If yes, in which situations?
	Law No. 9887, dated 10.03.2008 "On protection of personal data" in Article 7 thereof provides as one of the legal requirements for the processing of sensitive data, obtaining informed consent from the data subject which may be revoked at any given moment.
Withdrawal:	Are patients able to withdraw the consent given to EHR schemes? If yes, what is the relevant procedure to withdraw such consent? What are the consequences?
	Law No. 9887, dated 10.03.2008 "On protection of personal data" in Article 7/2 / or its states as one of the legal requirements for the processing of sensitive data, obtaining informed consent from the data subject which can be revoked at any given moment making illegal any further processing of data time.
Outsourcing processing of data:	Is outsourcing common? Under what circumstances? Where is the data outsourced to? What sort of safeguards are in place?
	Instruction Nr. 23, dated 20.11 2012 "Processing of personal data in the health sector", defines the health care provider may contract data processors for technical operations regarding the processing of health data (e.g. safe storage of data). In the case of using a data processor, the controller and the processor have to enter into a contract in writing, following the requirements the Law on protection of personal data and Instruction No. 19, dated 03.08.2012. The data processor shall follow the instructions of the health care provider when processing health data on behalf of it. It shall not use the data for its own purposes, and except where provided otherwise by law must not give third parties access to the data processed. The data processor must notify the controller if it intends to use other processors (sub-processors). In case of sub-processing, the requirements regarding the processor set out by the Law on protection of personal data and Instruction No. 19, dated 03.08.2012 must be applied even to the sub-processor.

2. Cloud Computing, Data Mining and Profiling from both Medical Records (including EHR) and Data not specifically related to medical records.

2.1. Data Protection Issues:

Cloud computing has brought a new dimension to the way data is stored, accessed and processed. Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS), Network as a service (NaaS) are all used by services and organisations that deal with both medical data and non-medical data.

With the development of more advanced and efficient data-mining and data-querying Medical techniques (e.g NoSQL, MapReduce, Hadoop) in conjunction with increased processing power and

data storage, mining data has never been more informative, easier, and cost-effective. Healthcare is a natural sector in which to apply new technologies and methodologies, with particular impacts in epidemiology, public health, health services research, etc. Data that can lead to the identification of a particular individual and his/her health situation is not limited to medical data *per se,* present on Electronic Health Records, but also to unsuspicious type of information. There is a growing concern that these schemes may be implemented in manner which does not always respect the patients' confidentiality and basic rights, and in a broader context, the use of this of information may prejudice the individuals concerned. The ability to track and monitor patients and resources enables a more efficient provision of care but may have an impact on the right to privacy of the individual concerned.

2.2. Questions: Is your legal framework providing for a regulation of Cloud Computing, Data Mining and Profiling? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	There is no specific legal regulation but Commissioner's Office has recently issued a guide (nonbinding) for the protection of personal data in cloud computing services.
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Cloud computing:	How is cloud computing regulated in your country? Which security safeguards and standards are mandatory? Are there specific requirements in order to store medical data in the cloud? How is data shared and is the sharing regulated?
	It is regulated by the guideline (nonbinding) to protect personal data in cloud computing services which provides rights and obligations of the client and service provider cloud Cloud
Government:	Do governmental programmes exist to allow for increased data-mining of medical records? If yes, what are the purposes of this data mining? Are private entities allowed to access the data? Under what circumstances? What sort of techniques and technologies are being used? To what end? Are data subjects informed of this type of data-mining?
	NA
Private sector:	Are private entities allowed to mine medical data which they process? Under what circumstances? Can the government have access to this data?
	NA
Profiling:	Are the government and the private sector allowed to employ profiling methods on medical data? If yes, under what circumstances? Is it allowed to cross and correlate non-medical data with medical data?

	NA

3. RFID and wireless communication technologies

3.1. Data Protection Issues:

It is common for medical devices, such as patients' tags, to possess RFID technologies in order to facilitate the transmission of the patients' data.

It can also be related to the data-mining operations previously mentioned as it is another category of information that can be used to discern meaningful patterns.

Transmission of data through radio-frequency is not limited to medical devices. Almost any smartphone uses some technology enabling to collect, and share, the user's data. For instance, via WI-FI it is possible to identify users' locations and therefore infer some of their behaviour, which in some cases can relate to health information.

3.2. Questions: Is your legal framework providing for a regulation of RFID technologies and the transfer of personal data through wireless technologies? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	It does not exist a specific regulation to RFID technologies. In the law on protection of personal data is there is the Article 27 which provides the "measures for the security of personal data" and Article 28 "Confidentiality of data". Controllers or processors, who do not take the data security measures and do not observe the duty to keep confidentiality, provided for under Articles 27 and 28 of this law, are fined from 10 000 ALL to 150 000 ALL.
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
RFID:	How is RFID used in hospital/clinics for (a) resource management, (b) patient care? What types of database systems (and security) are implemented in conjunction with RFID use? How are issues of access, sharing, consent etc. managed considering that RFID may be used without the patients' knowledge.
	NA
Wireless tracking technologies:	Are hospitals/clinics employing other wireless tracking technologies besides RFID? Which ones? Do they have to follow specific security requirements? Which ones?
	NA

4. Applications (Mobile)

4.1. Data Protection Issues:

Information society is increasingly relying on the use of "apps" (application), most of them mobile.

These apps are commonly designed to gather personal data, and in practice often process medical data. Technologies such as multi-touch touchscreen, accelerometers or gyroscopes, ambient light sensors, GPS and cameras, and devices featuring fingerprint and biometric sensors also involve the collection of medical data. A mobile phone application can monitor accurately physiological data, such as heartbeats, sleep patterns, fitness information.

4.2. Questions: Is your legal framework providing for a regulation of Apps and Mobile Apps? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	Our legal framework does not provide a special regulation for Apps and Mobile Apps. Regarding the general law, we mention Article 5 of the Law on the protection of personal data, which stipulates the general principles of protection of personal data and Article 7 on the criteria of processing sensitive data. Cases of data processing in contradiction with the provisions of this law do not constitute any criminal offence and are subject to a fine, are fined from 10 000 to 500 000 ALL.
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Apps:	Is it allowed to use apps and mobile apps to deploy medical services and collect medical data? If yes, which type of individual/organisation can develop and employ these apps? Are there specific security requirements for these types of apps?
Institutions:	Do hospitals/clinics/labs employ apps to gather medical data? Is there a need for a medical treatment to permit the use of an app to process the medical data? Are there specific security requirements for the institutions collecting these data from the apps? Are medico-administrative data used by hospitals/clinics for management purposes?
Tracking technologies:	Do hospitals/clinics/labs employ non-medical apps and devices to track and collect data from their patients? What type of data is collected? For what purpose? Is the data identifiable? Is the data combined with medical data?
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical apps and tracking apps? If yes, what are the standards?
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical diagnostic? How would this be applied to fitness and daily-basis data?

5. Medical Devices and Wearable Devices

5.1. Data Protection Issues:

A medical device can be defined as: 'any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application. Such a device should be intended by the manufacturer for one of a number of defined purposes, one of which is, diagnosis, prevention, monitoring, treatment or alleviation of disease' (Directive 93/42/EEC Article 1:2)

Some eHealth and mHealth devices and apps do not fall in this definition of medical devices, as can also be the case of a software working in combination with a physical device, for instance a smartphone.

5.2. Questions: Is your legal framework providing for a regulation of Medical Devices? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	Our legal framework does not provide a special regulation for Medical Devices. Regarding the general law, we mention Article 5 of the Law on the protection of personal data, which stipulates the general principles of protection of personal data and Article 7 on the criteria of processing sensitive data. Cases of data processing in contradiction with the provisions of this law do not constitute any criminal offence and are subject to a fine, are fined from 10 000 to 500 000 ALL.
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
eHealth and mHealth:	Does the concept of Medical device in your country encompass services and apparels in the realm of eHealth and mHealth? What are the requirements? Should, for instance, the medical device be certified before it can be used?
Apps:	Does the concept of medical devices encompass apps? If yes, is there any regulation applicable to apps that perform medical services? Is there any regulation applicable on apps that track non-medical data that can lead to health information? If yes, what type of data?
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical and/or wearable devices? If yes, what are the standards?
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical treatment? How would this be applied to fitness and daily-basis data?

6. Internet of Things

6.1. Data Protection Issues:

Internet of things relates to common, ordinary devices that are now, and increasingly, connected to the Internet, such as cars, fridges, ovens, microwaves, etc. All of these devices can provide data that can lead to reveal information concerning one's health. A fridge can easily inform on the type of food stored and thus the diet of an individual. One of the biggest challenges of the Internet of Things is to guarantee the right to privacy and data protection in a world where every device collects, processes, analyses and transmits the data, commonly via wireless technologies.

In the realm of medical data, the issue mainly arises when crossing seemly unrelated data that can lead to health information about an individual.

6.2. Questions: Is your legal framework providing for a regulation of the Internet of Things? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	Our legal framework does not provide a special regulation for Internet of Things. Regarding the general law, we mention Article 5 of the Law on the protection of personal data, which stipulates the general principles of protection of personal data and Article 7 on the criteria of processing sensitive data. Cases of data processing in contradiction with the provisions of this law do not constitute any criminal offence and are subject to a fine, are fined from 10 000 to 500 000 ALL. Also, article 27 which provide the "measures for the security of personal data" and Article 28 "Confidentiality of data". Controllers or processors, who do not take the data security measures and do not observe the duty to keep confidentiality, provided for under Articles 27 and 28 of this law, are fined from 10 000 ALL to 150 000 ALL.
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Security:	What are the security standards that need to be employed by these devices when collecting personal data?
Non-medical devices:	Are non-medical devices allowed to collect medical data, such as heart frequency? Are they allowed to cross medical data with non-medical data?
Privacy by Design:	Is there any requirement to implement privacy by design in the development of connected devices? If yes, what are the standards?

7. Electronic Doctor (online Doctor) and on-line appointments

7.1. Data Protection Issues:

The Doctor listens, talks and assesses the patient online, via a website, app, canal, sometimes

including video-conference. Medical data is collected and processed, what are the security requirements and standards followed? Other websites provide for on-line appointments with doctors, which can also involve the processing of medical data.

7.2. Questions: Is your legal framework providing for a regulation of online Medical Treatment and is the on-line appointment system covered by such a framework? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Medical treatment:	Is it allowed to perform medical treatment via online services? If yes, how should the medical services be provided? Does it have to follow the same requirements of a regular physically-present medical treatment?
Medical data:	How should the data collected via a medical treatment performed online be processed? Are there specific requirements? Which ones?

Other comments and technologies
Should you wish to describe any technology, feature or trend that has not been covered by the questionnaire, please feel free to use the space provided below. Where relevant, also indicate recent legislation changes, guidelines and/or case law.

ALBANIA / ALBANIE - AMERICAN HOSPITAL / HÔPITAL AMERICAIN

QUESTIONNAIRE

The questionnaire should ideally be completed by data protection authorities, health policy authorities, professional or patient associations as well as healthcare providers: you are invited to share it as widely as possible.

Please send your replies to dataprotection@coe.int no later than 15 December 2014.

1. Mobile Health (mHealth) and Electronic Health Records (EHR)

1.1. Data Protection Issues:

This is perhaps the biggest topic sitting at the intersection of technology and data protection. Mobile health (mHealth) and Electronic Health Records (EHR) are increasingly used in healthcare systems and provisions – it is a trend that needs to be examined.

Related to the EHR, these records are more accurate, cost-effective (in terms of storage) than paper-based notes. The concept of patient controlled/accessed EHR has been implemented in varying degrees in different countries.

Furthermore, some non-medical record can still contain health information about users and it should be considered if such records ought to be treated in a similar way to EHR.

Also, should 'medical data' as defined in Recommendation N° (97) 5 on the protection of medical data cover physical tracking data, such as pedometers or fitness data and data that can lead to medical information about an individual ?

1.2. Questions: if EHR exist in your country, is your legal framework providing for a regulation of such records? If mHealth exists in your country, is your legal framework providing for a specific regulation? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
EHR and Medical data:	What can be considered medical data in your country? Is it solely the data relating to a person's health (state, diagnosis, prognosis, medical treatment, etc.)? Is non-medical data that leads to medical information treated the same way as medical data (for instance in terms of confidentiality requirements)? Is the EHR solely constituted of data collected in a medical context or can the individual also himself or herself add information regarding his or her health?
	Information regarding the health of the person is considered health information. Non-health information are been treated as well, but not as the health information. EHR provides the individuals to enter the info regarding their health.
Sharing of data	Who is granted access to the EHR and how is the sharing of information (with

and Access:	other health care providers?) regulated? Where information is shared with pharmacists, is there a strict purpose limitation in place? How has the definition of the responsibility over the medical data been regulated?
	In EHR, has access only authorised staff based on the responds. Respective departments are responsible only for the information which is relevant to them.
Data quality:	Are the principles of legitimacy, fairness and minimisation applied to medical data? How are records kept accurate? How long is the data kept for, is the specific storage period defined for the EHR?
	Principle of legality for the patient data are kept partially. Accurate records are kept for an indefinite period.
Data integrity:	Are any specific methods used to ensure the integrity of the data? How are patients identified in the EHR? In the context of research, are anonymisation methods used and what safeguards exist for re-identification?
	To maintain the integrity of data, there are different standards used. Patients in EHR are identified by a no. Unique identification and personal data. No use of anonymisation.
Data security:	Where are the records stored? Is there a centralised database of EHR? What security technology is being used?
	The data are stored in a centralized database of EHR. Technology used is client-server and central database.
Rights of the person/patient concerned:	How can the right of access be exercised? How can the data be corrected? Can the person enter information in his or her own EHR? What are the legal remedies available?
	The rights of access are based on responsibilities. The data are corrected only by authorized staff and the persons cannot enter data about themselves or to retrieve them.
Consent:	Is the system based on an opt-in approach? Is the principle of granular consent applied (with the possibility of preventing access to certain data?)? If yes, in which situations?
Withdrawal:	Are patients able to withdraw the consent given to EHR schemes? If yes, what is the relevant procedure to withdraw such consent? What are the consequences?
	Patients do not have the right to withdraw the consent given in EHR schemes
Outsourcing processing of data:	Is outsourcing common? Under what circumstances? Where is the data outsourced to? What sort of safeguards are in place?
	We don’t use outsourcing.

2. Cloud Computing, Data Mining and Profiling from both Medical Records (including EHR) and Data not specifically related to medical records.

2.1. Data Protection Issues:

Cloud computing has brought a new dimension to the way data is stored, accessed and processed. Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS), Network as a service (NaaS) are all used by services and organisations that deal with both medical data and non-medical data.

With the development of more advanced and efficient data-mining and data-querying Medical techniques (e.g NoSQL, MapReduce, Hadoop) in conjunction with increased processing power and data storage, mining data has never been more informative, easier, and cost-effective.

Healthcare is a natural sector in which to apply new technologies and methodologies, with particular impacts in epidemiology, public health, health services research, etc.

Data that can lead to the identification of a particular individual and his/her health situation is not limited to medical data *per se,* present on Electronic Health Records, but also to unsuspicious type of information.

There is a growing concern that these schemes may be implemented in manner which does not always respect the patients' confidentiality and basic rights, and in a broader context, the use of this of information may prejudice the individuals concerned.

The ability to track and monitor patients and resources enables a more efficient provision of care but may have an impact on the right to privacy of the individual concerned.

2.2. Questions: Is your legal framework providing for a regulation of Cloud Computing, Data Mining and Profiling? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Cloud computing:	How is cloud computing regulated in your country? Which security safeguards and standards are mandatory? Are there specific requirements in order to store medical data in the cloud? How is data shared and is the sharing regulated?
	Cloud computing are provided by ISP, who use international safety standards. There are no specific criteria for the storage of medical data in the cloud. We don't have information distribution.
Government:	Do governmental programmes exist to allow for increased data-mining of medical records? If yes, what are the purposes of this data mining? Are private entities allowed to access the data? Under what circumstances? What sort of techniques and technologies are being used? To what end? Are data subjects informed of this type of data-mining?
	Don't have government programs that enable the growth of data mining.
Private sector:	Are private entities allowed to mine medical data which they process? Under what

	circumstances? Can the government have access to this data?
	Private entities are allowed to mine medical data for their internal effects, such as information, statistics etc. The government may have access to this information.
Profiling:	Are the government and the private sector allowed to employ profiling methods on medical data? If yes, under what circumstances? Is it allowed to cross and correlate non-medical data with medical data?
	Profiling methods can be used by the private sector for medical records but are not applicable.

3. RFID and wireless communication technologies

3.1. Data Protection Issues:

It is common for medical devices, such as patients' tags, to possess RFID technologies in order to facilitate the transmission of the patients' data.

It can also be related to the data-mining operations previously mentioned as it is another category of information that can be used to discern meaningful patterns.

Transmission of data through radio-frequency is not limited to medical devices. Almost any smartphone uses some technology enabling to collect, and share, the user's data. For instance, via WI-FI it is possible to identify users' locations and therefore infer some of their behaviour, which in some cases can relate to health information.

3.2. Questions: Is your legal framework providing for a regulation of RFID technologies and the transfer of personal data through wireless technologies? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
RFID:	How is RFID used in hospital/clinics for (a) resource management, (b) patient care? What types of database systems (and security) are implemented in conjunction with RFID use? How are issues of access, sharing, consent etc. managed considering that RFID may be used without the patients' knowledge.
	RFID is not used to manage the data. If it is used, will be only for internal connections and apply security standards (such as password and encryption). Access is granted only to authorize internal staff.
Wireless tracking technologies:	Are hospitals/clinics employing other wireless tracking technologies besides RFID? Which ones? Do they have to follow specific security requirements? Which ones?
	We don't use wireless tracking technology

4. Applications (Mobile)

4.1. Data Protection Issues:

Information society is increasingly relying on the use of "apps" (application), most of them mobile. These apps are commonly designed to gather personal data, and in practice often process medical data.
Technologies such as multi-touch touchscreen, accelerometers or gyroscopes, ambient light sensors, GPS and cameras, and devices featuring fingerprint and biometric sensors also involve the collection of medical data.

A mobile phone application can monitor accurately physiological data, such as heartbeats, sleep patterns, fitness information.

4.2. Questions: Is your legal framework providing for a regulation of Apps and Mobile Apps? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Apps:	Is it allowed to use apps and mobile apps to deploy medical services and collect medical data? If yes, which type of individual/organisation can develop and employ these apps? Are there specific security requirements for these types of apps?
	It is allowed the use of apps for medical services and medical data collection. Only internal staff or contracting firm has the right to develop the program based on demand and only internal staff has the right to use it. There are specific requirements for different levels of security.
Institutions:	Do hospitals/clinics/labs employ apps to gather medical data? Is there a need for a medical treatment to permit the use of an app to process the medical data? Are there specific security requirements for the institutions collecting these data from the apps? Are medico-administrative data used by hospitals/clinics for management purposes?
	Hospital uses the app to collect medical data. Often medical treatment requires the use of the app to process medical records. There are special security requests for this information from institutions. The data are used by hospital for management purposes.
Tracking technologies:	Do hospitals/clinics/labs employ non-medical apps and devices to track and collect data from their patients? What type of data is collected? For what purpose? Is the data identifiable? Is the data combined with medical data?
	No other app are used to collect data from patients
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical apps and tracking apps? If yes, what are the standards?

	Yes, there is a request for implementing Privacy by Design in the development of medical applications by the staff and internal departments. We are not using any specific standard for this purpose.
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical diagnostic? How would this be applied to fitness and daily-basis data?
	The system is not based on an approach opt-in or opt-out.

5. Medical Devices and Wearable Devices

5.1. Data Protection Issues:

A medical device can be defined as: 'any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application. Such a device should be intended by the manufacturer for one of a number of defined purposes, one of which is, diagnosis, prevention, monitoring, treatment or alleviation of disease' (Directive 93/42/EEC Article 1:2)

Some eHealth and mHealth devices and apps do not fall in this definition of medical devices, as can also be the case of a software working in combination with a physical device, for instance a smartphone.

5.2. Questions: Is your legal framework providing for a regulation of Medical Devices? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
eHealth and mHealth:	Does the concept of Medical device in your country encompass services and apparels in the realm of eHealth and mHealth? What are the requirements? Should, for instance, the medical device be certified before it can be used?
	No, is not applicable.
Apps:	Does the concept of medical devices encompass apps? If yes, is there any regulation applicable to apps that perform medical services? Is there any regulation applicable on apps that track non-medical data that can lead to health information? If yes, what type of data?
	Yes, includes applications that are used by equipment from special medical dpt. There are not used to track non-medical information.

Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical and/or wearable devices? If yes, what are the standards?
	There are requirement to implement the development of PbD in medical equipment but based on the standards of the medical device.
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical treatment? How would this be applied to fitness and daily-basis data?
	The system is not based on an opt-out approach.

6. Internet of Things

6.1. Data Protection Issues:

Internet of things relates to common, ordinary devices that are now, and increasingly, connected to the Internet, such as cars, fridges, ovens, microwaves, etc. All of these devices can provide data that can lead to reveal information concerning one's health. A fridge can easily inform on the type of food stored and thus the diet of an individual. One of the biggest challenges of the Internet of Things is to guarantee the right to privacy and data protection in a world where every device collects, processes, analyses and transmits the data, commonly via wireless technologies.

In the realm of medical data, the issue mainly arises when crossing seemly unrelated data that can lead to health information about an individual.

6.2. Questions: Is your legal framework providing for a regulation of the Internet of Things? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Security:	What are the security standards that need to be employed by these devices when collecting personal data?
	There are not standard used by these devices.
Non-medical devices:	Are non-medical devices allowed to collect medical data, such as heart frequency? Are they allowed to cross medical data with non-medical data?
	Is not allowed the non-medical equipment to collect medical records or data crossing with medical devices.
Privacy by Design:	Is there any requirement to implement privacy by design in the development of connected devices? If yes, what are the standards?

	There is no requirement for the implementation of the PbD for these devices.

7. Electronic Doctor (online Doctor) and on-line appointments

7.1. Data Protection Issues:

The Doctor listens, talks and assesses the patient online, via a website, app, canal, sometimes including video-conference. Medical data is collected and processed, what are the security requirements and standards followed? Other websites provide for on-line appointments with doctors, which can also involve the processing of medical data.

7.2. Questions: Is your legal framework providing for a regulation of online Medical Treatment and is the on-line appointment system covered by such a framework? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Medical treatment:	Is it allowed to perform medical treatment via online services? If yes, how should the medical services be provided? Does it have to follow the same requirements of a regular physically-present medical treatment?
	No, is not allowed medical treatment services through online, only consultancy.
Medical data:	How should the data collected via a medical treatment performed online be processed? Are there specific requirements? Which ones?
	The data must be processed in different structures for different cases in order to become an elaboration as precise information that comes online. This can be done in three steps, gathering information that should be precise, its processing in the appropriate way for each case and at the end of its analysis in order to identify arguments can and techniques.

Other comments and technologies
Should you wish to describe any technology, feature or trend that has not been covered by the questionnaire, please feel free to use the space provided below. Where relevant, also indicate recent legislation changes, guidelines and/or case law.

ALBANIA / ALBANIE - SALUS HOSPITAL / HÔPITAL SALUS

QUESTIONNAIRE

The questionnaire should ideally be completed by data protection authorities, health policy authorities, professional or patient associations as well as healthcare providers: you are invited to share it as widely as possible.

Please send your replies to dataprotection@coe.int no later than 15 December 2014.

1. Mobile Health (mHealth) and Electronic Health Records (EHR)

1.1. Data Protection Issues:

This is perhaps the biggest topic sitting at the intersection of technology and data protection. Mobile health (mHealth) and Electronic Health Records (EHR) are increasingly used in healthcare systems and provisions – it is a trend that needs to be examined.

Related to the EHR, these records are more accurate, cost-effective (in terms of storage) than paper-based notes. The concept of patient controlled/accessed EHR has been implemented in varying degrees in different countries.

Furthermore, some non-medical record can still contain health information about users and it should be considered if such records ought to be treated in a similar way to EHR.

Also, should 'medical data' as defined in Recommendation N° (97) 5 on the protection of medical data cover physical tracking data, such as pedometers or fitness data and data that can lead to medical information about an individual ?

1.2. Questions: if EHR exist in your country, is your legal framework providing for a regulation of such records? If mHealth exists in your country, is your legal framework providing for a specific regulation? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	We not have a law that discipline electronic health records. Salus have installed a program that manages electronic patient records (Medarchiver). Currently we are aware of only apparently legal reference for the protection of personal data medical is a law number 9887 date 10.03.2008.
Case-law:	Don't have
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
EHR and Medical data:	What can be considered medical data in your country? Is it solely the data relating to a person's health (state, diagnosis, prognosis, medical treatment, etc.)? Is non-medical data that leads to medical information treated the same way as medical data (for instance in terms of confidentiality requirements)? Is the EHR solely constituted of data collected in a medical context or can the individual also himself or herself add information regarding his or her health?

	The data which determinat condition, diagnosis, prognosis, medical treatment. For the protection of personal data and confidentiality for more than 90% of the services offered. It is impossible for the patient to add information about her or his health.
Sharing of data and Access:	Who is granted access to the EHR and how is the sharing of information (with other health care providers?) regulated? Where information is shared with pharmacists, is there a strict purpose limitation in place? How has the definition of the responsibility over the medical data been regulated?
	All employees who are related to medical treatment and financial treatment. The information is not shared with the pharmacist. Every doctor who treats the patient has access to the EHR as informed about the history of the patient. Our system give the possibility to restrict the access.
Data quality:	Are the principles of legitimacy, fairness and minimisation applied to medical data? How are records kept accurate? How long is the data kept for, is the specific storage period defined for the EHR?
	We apply the principles of legitimacy, fairness and minimization. Technically there is no loss off data we reserve at 100%. The data will never cancelled, delete, we conserve an eternity.
Data integrity:	Are any specific methods used to ensure the integrity of the data? How are patients identified in the EHR? In the context of research, are anonymisation methods used and what safeguards exist for re-identification?
	No, we don't have a particular methods. The patients are identificate by name and surname always. Electronically such methods do not exist.
Data security:	Where are the records stored? Is there a centralised database of EHR? What security technology is being used?
	In the database. There is a centralized database. Technology security user authentication with username and password.
Rights of the person/patient concerned:	How can the right of access be exercised? How can the data be corrected? Can the person enter information in his or her own EHR? What are the legal remedies available?
	By using Username and Password. Medical records can be changed only by the medical referring. No absolutely any person can't make any information in the EHR. Law for the protection of personal data.
Consent:	Is the system based on an opt-in approach? Is the principle of granular consent applied (with the possibility of preventing access to certain data?)? If yes, in which situations?
	The system is based on an opt-in approach. only authorized persons have access.

Withdrawal:	Are patients able to withdraw the consent given to EHR schemes? If yes, what is the relevant procedure to withdraw such consent? What are the consequences?
	Patient consent form is extracted from the EHR and they shall sign. We give copy of the consent of the patient.
Outsourcing processing of data:	Is outsourcing common? Under what circumstances? Where is the data outsourced to? What sort of safeguards are in place?
	We not applicate subcontracting.

2. Cloud Computing, Data Mining and Profiling from both Medical Records (including EHR) and Data not specifically related to medical records.

2.1. Data Protection Issues:

Cloud computing has brought a new dimension to the way data is stored, accessed and processed. Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS), Network as a service (NaaS) are all used by services and organisations that deal with both medical data and non-medical data.

With the development of more advanced and efficient data-mining and data-querying Medical techniques (e.g NoSQL, MapReduce, Hadoop) in conjunction with increased processing power and data storage, mining data has never been more informative, easier, and cost-effective.

Healthcare is a natural sector in which to apply new technologies and methodologies, with particular impacts in epidemiology, public health, health services research, etc.

Data that can lead to the identification of a particular individual and his/her health situation is not limited to medical data *per se,* present on Electronic Health Records, but also to unsuspicious type of information.

There is a growing concern that these schemes may be implemented in manner which does not always respect the patients' confidentiality and basic rights, and in a broader context, the use of this of information may prejudice the individuals concerned.

The ability to track and monitor patients and resources enables a more efficient provision of care but may have an impact on the right to privacy of the individual concerned.

2.2. Questions: Is your legal framework providing for a regulation of Cloud Computing, Data Mining and Profiling? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	Don't provide
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Cloud computing:	How is cloud computing regulated in your country? Which security safeguards and standards are mandatory? Are there specific requirements in order to store

	medical data in the cloud? How is data shared and is the sharing regulated?
	Cloud computing does not exist in our country.
Government:	Do governmental programmes exist to allow for increased data-mining of medical records? If yes, what are the purposes of this data mining? Are private entities allowed to access the data? Under what circumstances? What sort of techniques and technologies are being used? To what end? Are data subjects informed of this type of data-mining?
	There are no government programs to enable increased data-mining medical data.
Private sector:	Are private entities allowed to mine medical data which they process? Under what circumstances? Can the government have access to this data?
	In our hospital we don't have data mine. Only article 7 of Law n. 9887 dated 10.03.2008 allows processing: Processing of sensitive data, in circumstances other than those specified in paragraph 2 of this article, is regulated by the Council of Ministers, only for purposes of important public interests, under appropriate protective measures.
Profiling:	Are the government and the private sector allowed to employ profiling methods on medical data? If yes, under what circumstances? Is it allowed to cross and correlate non-medical data with medical data?
	The only legal reference for the protection of personal data is LAW No. 9887, dated 10.3.2008, LAW FOR THE PROTECTION OF PERSONAL DATA, and Article 7 " The data required for the purposes of preventive medicine, medical diagnosis, the provision of health care, treatment, and management of health care services and their use by medical personnel or other persons who have the obligation of confidentiality.

3. RFID and wireless communication technologies

3.1. Data Protection Issues:

It is common for medical devices, such as patients' tags, to possess RFID technologies in order to facilitate the transmission of the patients' data.

It can also be related to the data-mining operations previously mentioned as it is another category of information that can be used to discern meaningful patterns.

Transmission of data through radio-frequency is not limited to medical devices. Almost any smartphone uses some technology enabling to collect, and share, the user's data. For instance, via WI-FI it is possible to identify users' locations and therefore infer some of their behaviour, which in some cases can relate to health information.

3.2. Questions: Is your legal framework providing for a regulation of RFID technologies and the transfer of personal data through wireless technologies? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged

in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	The legal does not provide for an adjustment for RFID technologies. We do not use as.
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
RFID:	How is RFID used in hospital/clinics for (a) resource management, (b) patient care? What types of database systems (and security) are implemented in conjunction with RFID use? How are issues of access, sharing, consent etc. managed considering that RFID may be used without the patients' knowledge.
	We don't use.
Wireless tracking technologies:	Are hospitals/clinics employing other wireless tracking technologies besides RFID? Which ones? Do they have to follow specific security requirements? Which ones?
	We do not apply as other structure.

4. Applications (Mobile)

4.1. Data Protection Issues:

Information society is increasingly relying on the use of "apps" (application), most of them mobile. These apps are commonly designed to gather personal data, and in practice often process medical data.
Technologies such as multi-touch touchscreen, accelerometers or gyroscopes, ambient light sensors, GPS and cameras, and devices featuring fingerprint and biometric sensors also involve the collection of medical data.

A mobile phone application can monitor accurately physiological data, such as heartbeats, sleep patterns, fitness information.

4.2. Questions: Is your legal framework providing for a regulation of Apps and Mobile Apps? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	Don't have legal prediction.
Case-law:	Don't have
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Apps:	Is it allowed to use apps and mobile apps to deploy medical services and collect medical data? If yes, which type of individual/organisation can develop and employ these apps? Are there specific security requirements for these types of apps?
	Our structures don't use these applications.

Institutions:	Do hospitals/clinics/labs employ apps to gather medical data? Is there a need for a medical treatment to permit the use of an app to process the medical data? Are there specific security requirements for the institutions collecting these data from the apps? Are medico-administrative data used by hospitals/clinics for management purposes?
	Our structures don't use these applications to collect medical data. The data used for management purposes in the context of quality improvement.
Tracking technologies:	Do hospitals/clinics/labs employ non-medical apps and devices to track and collect data from their patients? What type of data is collected? For what purpose? Is the data identifiable? Is the data combined with medical data?
	Our structure does not use non- medical app
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical apps and tracking apps? If yes, what are the standards?
	Our structure does not use non- medical app
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical diagnostic? How would this be applied to fitness and daily-basis data?
	We do not use structure as non-medical applications and equipment for tracking and collecting data from their patients

5. Medical Devices and Wearable Devices

5.1. Data Protection Issues:

A medical device can be defined as: 'any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application. Such a device should be intended by the manufacturer for one of a number of defined purposes, one of which is, diagnosis, prevention, monitoring, treatment or alleviation of disease' (Directive 93/42/EEC Article 1:2)

Some eHealth and mHealth devices and apps do not fall in this definition of medical devices, as can also be the case of a software working in combination with a physical device, for instance a smartphone.

5.2. Questions: Is your legal framework providing for a regulation of Medical Devices? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	There is no specific law for this. For medical equipment becomes simply the service and technical control.
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).

eHealth and mHealth:	Does the concept of Medical device in your country encompass services and apparels in the realm of eHealth and mHealth? What are the requirements? Should, for instance, the medical device be certified before it can be used?
	Not include
Apps:	Does the concept of medical devices encompass apps? If yes, is there any regulation applicable to apps that perform medical services? Is there any regulation applicable on apps that track non-medical data that can lead to health information? If yes, what type of data?
	No.
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical and/or wearable devices? If yes, what are the standards?
	Not include
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical treatment? How would this be applied to fitness and daily-basis data?
	Not include

6. Internet of Things

6.1. Data Protection Issues:

Internet of things relates to common, ordinary devices that are now, and increasingly, connected to the Internet, such as cars, fridges, ovens, microwaves, etc. All of these devices can provide data that can lead to reveal information concerning one's health. A fridge can easily inform on the type of food stored and thus the diet of an individual. One of the biggest challenges of the Internet of Things is to guarantee the right to privacy and data protection in a world where every device collects, processes, analyses and transmits the data, commonly via wireless technologies.

In the realm of medical data, the issue mainly arises when crossing seemly unrelated data that can lead to health information about an individual.

6.2. Questions: Is your legal framework providing for a regulation of the Internet of Things? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	No there is a legal reference
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Security:	What are the security standards that need to be employed by these devices when collecting personal data?
	We don't use these devices

Non-medical devices:	Are non-medical devices allowed to collect medical data, such as heart frequency? Are they allowed to cross medical data with non-medical data?
	We don't have a non- medical devices
Privacy by Design:	Is there any requirement to implement privacy by design in the development of connected devices? If yes, what are the standards?
	No there is any requirement

7. Electronic Doctor (online Doctor) and on-line appointments

7.1. Data Protection Issues:

The Doctor listens, talks and assesses the patient online, via a website, app, canal, sometimes including video-conference. Medical data is collected and processed, what are the security requirements and standards followed? Other websites provide for on-line appointments with doctors, which can also involve the processing of medical data.

7.2. Questions: Is your legal framework providing for a regulation of online Medical Treatment and is the on-line appointment system covered by such a framework? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	No there is a legal reference
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Medical treatment:	Is it allowed to perform medical treatment via online services? If yes, how should the medical services be provided? Does it have to follow the same requirements of a regular physically-present medical treatment?
	It is allowed. The same requirement.
Medical data:	How should the data collected via a medical treatment performed online be processed? Are there specific requirements? Which ones?
	No there are no specific requirements for processing. Operated by law for the protection of personal data in Article 7: Processing of sensitive data, in circumstances other than those specified in paragraph 2 of this article, is regulated by the Council of Ministers, only for purposes of important public interests, under appropriate protective measures.

Other comments and technologies
Should you wish to describe any technology, feature or trend that has not been covered by the questionnaire, please feel free to use the space provided below. Where relevant, also indicate recent legislation changes, guidelines and/or case law.

ALBANIA / ALBANIE - UNIVERSITY HOSPITAL CENTER "MOTHER THERESA"

QUESTIONNAIRE

The questionnaire should ideally be completed by data protection authorities, health policy authorities, professional or patient associations as well as healthcare providers: you are invited to share it as widely as possible.

Please send your replies to dataprotection@coe.int no later than 15 December 2014.

1. Mobile Health (mHealth) and Electronic Health Records (EHR)

1.1. Data Protection Issues:

This is perhaps the biggest topic sitting at the intersection of technology and data protection. Mobile health (mHealth) and Electronic Health Records (EHR) are increasingly used in healthcare systems and provisions – it is a trend that needs to be examined.

Related to the EHR, these records are more accurate, cost-effective (in terms of storage) than paper-based notes. The concept of patient controlled/accessed EHR has been implemented in varying degrees in different countries.

Furthermore, some non-medical record can still contain health information about users and it should be considered if such records ought to be treated in a similar way to EHR.

Also, should 'medical data' as defined in Recommendation N° (97) 5 on the protection of medical data cover physical tracking data, such as pedometers or fitness data and data that can lead to medical information about an individual ?

1.2. Questions: if EHR exist in your country, is your legal framework providing for a regulation of such records? If mHealth exists in your country, is your legal framework providing for a specific regulation? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	
Case-law:	No
Other:	No

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
EHR and Medical data:	What can be considered medical data in your country? Is it solely the data relating to a person's health (state, diagnosis, prognosis, medical treatment, etc.)? Is non-medical data that leads to medical information treated the same way as medical data (for instance in terms of confidentiality requirements)? Is the EHR solely constituted of data collected in a medical context or can the individual also himself or herself add information regarding his or her health?

	Medical data in our country are considered: state, diagnosis, prognosis and medical treatment. These medical data are treated the same way as confidential data. EHR is solely constituted of data collected in a medical context. An individual can not add information.
Sharing of data and Access:	Who is granted access to the EHR and how is the sharing of information (with other health care providers?) regulated? Where information is shared with pharmacists, is there a strict purpose limitation in place? How has the definition of the responsibility over the medical data been regulated?
	The medical staff has access to the medical data. There is a limit information given to the pharmacists. The responsibility over the medical data has been regulated by signing a Privacy Statement.
Data quality:	Are the principles of legitimacy, fairness and minimisation applied to medical data? How are records kept accurate? How long is the data kept for, is the specific storage period defined for the EHR?
	Yes, the principles of legitimacy, fairness and minimization are applied for the medical data. The data is kept for a non- specified period of time.
Data integrity:	Are any specific methods used to ensure the integrity of the data? How are patients identified in the EHR? In the context of research, are anonymisation methods used and what safeguards exist for re-identification?
	No, there are not specific methods. The patients are identified by their names, surnames, ID card or ID passport. Safeguards are the access levels to the medical data.
Data security:	Where are the records stored? Is there a centralised database of EHR? What security technology is being used?
	There is a database which is centralized.
Rights of the person/patient concerned:	How can the right of access be exercised? How can the data be corrected? Can the person enter information in his or her own EHR? What are the legal remedies available?
	The data can not be corrected. Even if they are corrected, traces remain in the system. An individual can not enter information on his/her own.
Consent:	Is the system based on an opt-in approach? Is the principle of granular consent applied (with the possibility of preventing access to certain data?)? If yes, in which situations?
	Yes, the access to certain data can be prevented by activation or non- activation in data entry.
Withdrawal:	Are patients able to withdraw the consent given to EHR schemes? If yes, what is the relevant procedure to withdraw such consent? What are the consequences?
Outsourcing processing of	Is outsourcing common? Under what circumstances? Where is the data outsourced to? What sort of safeguards are in place?

data:	Not applicable.

2. Cloud Computing, Data Mining and Profiling from both Medical Records (including EHR) and Data not specifically related to medical records.

2.1. Data Protection Issues:

Cloud computing has brought a new dimension to the way data is stored, accessed and processed. Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS), Network as a service (NaaS) are all used by services and organisations that deal with both medical data and non-medical data.

With the development of more advanced and efficient data-mining and data-querying Medical techniques (e.g NoSQL, MapReduce, Hadoop) in conjunction with increased processing power and data storage, mining data has never been more informative, easier, and cost-effective.

Healthcare is a natural sector in which to apply new technologies and methodologies, with particular impacts in epidemiology, public health, health services research, etc.

Data that can lead to the identification of a particular individual and his/her health situation is not limited to medical data *per se,* present on Electronic Health Records, but also to unsuspicious type of information.

There is a growing concern that these schemes may be implemented in manner which does not always respect the patients' confidentiality and basic rights, and in a broader context, the use of this of information may prejudice the individuals concerned.

The ability to track and monitor patients and resources enables a more efficient provision of care but may have an impact on the right to privacy of the individual concerned.

2.2. Questions: Is your legal framework providing for a regulation of Cloud Computing, Data Mining and Profiling? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	
Case-law:	No
Other:	No

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Cloud computing:	How is cloud computing regulated in your country? Which security safeguards and standards are mandatory? Are there specific requirements in order to store medical data in the cloud? How is data shared and is the sharing regulated?
	We don't have cloud computing in our institution.
Government:	Do governmental programmes exist to allow for increased data-mining of medical records? If yes, what are the purposes of this data mining? Are private entities allowed to access the data? Under what circumstances? What sort of techniques and technologies are being used? To what end? Are data subjects informed of this type of data-mining?

	We are not aware of government programs.
Private sector:	Are private entities allowed to mine medical data which they process? Under what circumstances? Can the government have access to this data?
	We don't have information about that.
Profiling:	Are the government and the private sector allowed to employ profiling methods on medical data? If yes, under what circumstances? Is it allowed to cross and correlate non-medical data with medical data?
	We don't have information about that.

3. RFID and wireless communication technologies

3.1. Data Protection Issues:

It is common for medical devices, such as patients' tags, to possess RFID technologies in order to facilitate the transmission of the patients' data.

It can also be related to the data-mining operations previously mentioned as it is another category of information that can be used to discern meaningful patterns.

Transmission of data through radio-frequency is not limited to medical devices. Almost any smartphone uses some technology enabling to collect, and share, the user's data. For instance, via WI-FI it is possible to identify users' locations and therefore infer some of their behaviour, which in some cases can relate to health information.

3.2. Questions: Is your legal framework providing for a regulation of RFID technologies and the transfer of personal data through wireless technologies? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	
Case-law:	No
Other:	No

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
RFID:	How is RFID used in hospital/clinics for (a) resource management, (b) patient care? What types of database systems (and security) are implemented in conjunction with RFID use? How are issues of access, sharing, consent etc. managed considering that RFID may be used without the patients' knowledge.
	Is not used.
Wireless tracking technologies:	Are hospitals/clinics employing other wireless tracking technologies besides RFID? Which ones? Do they have to follow specific security requirements? Which ones?
	Is not used.

4. Applications (Mobile)

4.1. Data Protection Issues:

Information society is increasingly relying on the use of “apps” (application), most of them mobile. These apps are commonly designed to gather personal data, and in practice often process medical data.
Technologies such as multi-touch touchscreen, accelerometers or gyroscopes, ambient light sensors, GPS and cameras, and devices featuring fingerprint and biometric sensors also involve the collection of medical data.

A mobile phone application can monitor accurately physiological data, such as heartbeats, sleep patterns, fitness information.

4.2. Questions: Is your legal framework providing for a regulation of Apps and Mobile Apps? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs’ opinions and/or case law.

Legislation:	
Case-law:	No
Other:	No

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs’ opinions and/or case law).	
Apps:	Is it allowed to use apps and mobile apps to deploy medical services and collect medical data? If yes, which type of individual/organisation can develop and employ these apps? Are there specific security requirements for these types of apps?
	We are not aware.
Institutions:	Do hospitals/clinics/labs employ apps to gather medical data? Is there a need for a medical treatment to permit the use of an app to process the medical data? Are there specific security requirements for the institutions collecting these data from the apps? Are medico-administrative data used by hospitals/clinics for management purposes?
	We do not use.
Tracking technologies:	Do hospitals/clinics/labs employ non-medical apps and devices to track and collect data from their patients? What type of data is collected? For what purpose? Is the data identifiable? Is the data combined with medical data?
	No, we do not use other technologies.
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical apps and tracking apps? If yes, what are the standards?
	No.
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical diagnostic? How would this be applied to fitness and daily-basis data?

	We do not understand that.

5. Medical Devices and Wearable Devices

5.1. Data Protection Issues:

A medical device can be defined as: 'any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application. Such a device should be intended by the manufacturer for one of a number of defined purposes, one of which is, diagnosis, prevention, monitoring, treatment or alleviation of disease' (Directive 93/42/EEC Article 1:2)

Some eHealth and mHealth devices and apps do not fall in this definition of medical devices, as can also be the case of a software working in combination with a physical device, for instance a smartphone.

5.2. Questions: Is your legal framework providing for a regulation of Medical Devices? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	
Case-law:	No
Other:	No

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
eHealth and mHealth:	Does the concept of Medical device in your country encompass services and apparels in the realm of eHealth and mHealth? What are the requirements? Should, for instance, the medical device be certified before it can be used?
	Medical device must be certified before being used. .
Apps:	Does the concept of medical devices encompass apps? If yes, is there any regulation applicable to apps that perform medical services? Is there any regulation applicable on apps that track non-medical data that can lead to health information? If yes, what type of data?
	Apps do not belong to the concept of medical equipment. There is no regulation.
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical and/or wearable devices? If yes, what are the standards?
	No, there is not.
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical treatment? How would this be applied to fitness and daily-basis data?
	We do not understand that.

6. Internet of Things

6.1. Data Protection Issues:

Internet of things relates to common, ordinary devices that are now, and increasingly, connected to the Internet, such as cars, fridges, ovens, microwaves, etc. All of these devices can provide data that can lead to reveal information concerning one's health. A fridge can easily inform on the type of food stored and thus the diet of an individual. One of the biggest challenges of the Internet of Things is to guarantee the right to privacy and data protection in a world where every device collects, processes, analyses and transmits the data, commonly via wireless technologies.

In the realm of medical data, the issue mainly arises when crossing seemly unrelated data that can lead to health information about an individual.

6.2. Questions: Is your legal framework providing for a regulation of the Internet of Things? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	
Case-law:	No
Other:	No

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Security:	What are the security standards that need to be employed by these devices when collecting personal data?
	ISO standards provided by the manufacturer.
Non-medical devices:	Are non-medical devices allowed to collect medical data, such as heart frequency? Are they allowed to cross medical data with non-medical data?
	Are not allowed.
Privacy by Design:	Is there any requirement to implement privacy by design in the development of connected devices? If yes, what are the standards?
	No there is not.

7. Electronic Doctor (online Doctor) and on-line appointments

7.1. Data Protection Issues:

The Doctor listens, talks and assesses the patient online, via a website, app, canal, sometimes including video-conference. Medical data is collected and processed, what are the security requirements and standards followed? Other websites provide for on-line appointments with doctors, which can also involve the processing of medical data.

7.2. Questions: Is your legal framework providing for a regulation of online Medical Treatment and is the on-line appointment system covered by such a framework? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions

envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	
Case-law:	No
Other:	No

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Medical treatment:	Is it allowed to perform medical treatment via online services? If yes, how should the medical services be provided? Does it have to follow the same requirements of a regular physically-present medical treatment?
	Medical treatment via online services are not applied.
Medical data:	How should the data collected via a medical treatment performed online be processed? Are there specific requirements? Which ones?
	We do not collect data via online services.

Other comments and technologies
Should you wish to describe any technology, feature or trend that has not been covered by the questionnaire, please feel free to use the space provided below. Where relevant, also indicate recent legislation changes, guidelines and/or case law.

AUSTRIA / AUTRICHE

QUESTIONNAIRE

The questionnaire should ideally be completed by data protection authorities, health policy authorities, professional or patient associations as well as healthcare providers: you are invited to share it as widely as possible.

Please send your replies to dataprotection@coe.int no later than 15 December 2014.

1. Mobile Health (mHealth) and Electronic Health Records (EHR)

1.1. Data Protection Issues:

This is perhaps the biggest topic sitting at the intersection of technology and data protection. Mobile health (mHealth) and Electronic Health Records (EHR) are increasingly used in healthcare systems and provisions – it is a trend that needs to be examined.

Related to the EHR, these records are more accurate, cost-effective (in terms of storage) than paper-based notes. The concept of patient controlled/accessed EHR has been implemented in varying degrees in different countries.

Furthermore, some non-medical record can still contain health information about users and it should be considered if such records ought to be treated in a similar way to EHR.

Also, should 'medical data' as defined in Recommendation N° (97) 5 on the protection of medical data cover physical tracking data, such as pedometers or fitness data and data that can lead to medical information about an individual ?

1.2. Questions: if EHR exist in your country, is your legal framework providing for a regulation of such records? If mHealth exists in your country, is your legal framework providing for a specific regulation? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	EHR in Austria: The electronic health record in Austria is as to date -still under construction. The nine provinces (Bundesländer), social security and the federal entity (Republic of Austria) have committed themselves to create and implement the so called **ELGA** (acronym for EHR in Austria) on a joint basis. The Electronic Health Record Act 2012 (EHRA 2012; available (in German and English) online at http://www.ris.bka.gv.at/Dokumente/Erv/ERV_2012_1_111/ERV_2012_1_111.pdf) entered into force on January 1st, 2013 and provides the legal basis for the implementation of the central components of ELGA as well as the specification of health care providers and health data to be processed within the ELGA system. mHealth: There is no state driven mHealth project comparable to ELGA. Text services (for appointments, reminders, etc.) as well as health oriented apps are offered by some health care providers. These have to comply with the provisions of the Health Telematics Act and the Data Protection Act 2000 (DPA 2000; available in English at http://www.dsb.gv.at/site/6274/default.aspx).

	The Data Protection Authority provides specific information on ELGA on its website (http://www.dsb.gv.at/site/8157/default.aspx).
Case-law:	To date, there is no final case law on EHR.
Other:	----------

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
EHR and Medical data:	What can be considered medical data in your country? Is it solely the data relating to a person's health (state, diagnosis, prognosis, medical treatment, etc.)? Is non-medical data that leads to medical information treated the same way as medical data (for instance in terms of confidentiality requirements)? Is the EHR solely constituted of data collected in a medical context or can the individual also himself or herself add information regarding his or her health?
	Medical data: According to § 4/2 DPA 2000, health data contain information about a person's health state. The EHRA 2012 leaves this provision untouched and defines Medical data as "Health Data" in § 2/1 EHRA 2012. There is an additional definition in § 2/9 EHRA 2012 of "EHR-Health Data" which may legally be used in the Austrian EHR. Thus, the EHR is solely constituted of data which are created in a medical context exclusively by health professionals. Non-medical data: Non-medical data that leads to medical information is treated in the same way when it comes e.g. to confidentiality issues at the workplace (e.g. a visit of a specific website that might lead to certain conclusions concerning a person's condition).
Sharing of data and Access:	Who is granted access to the EHR and how is the sharing of information (with other health care providers?) regulated? Where information is shared with pharmacists, is there a strict purpose limitation in place? How has the definition of the responsibility over the medical data been regulated?
	Access to the EHR and sharing of information: The legal access to ELGA is based on the principles of role and identity, i.e. only those health care providers who are listed in a special index, whose identity is proven by this index and who act according to their legally defined role (e.g. general practitioner) are allowed to retrieve patient data by means of ELGA. See § 2/10 EHRA 2012. Access is provided by way of the "Access Control Centre" (§ 2/10 in conjunction with § 21/2 EHRA 2012). Pharmacists: Pharmacists are by definition of § 2/10/c EHR-HCPs. Their access rights are, however, subject to a time limit of two hours after the last identification of the patient (physical contact) and only for medication data ("e-Medikation"). Responsibility for medical data: The existing rules concerning statutory documentation requirements and responsibility for the medical data of practitioners, hospitals and pharmacists (i.e. ÄrzteG, Apothekerordnung, Kranken- und Kuranstaltengesetz) remain untouched by ELGA.
Data quality:	Are the principles of legitimacy, fairness and minimisation applied to medical data? How records are kept accurate? How long is the data kept for, is the specific storage period defined for the EHR?
	Principles of legitimacy, fairness and minimization: The principles of legitimacy, fairness and minimisation apply to medical data according to § 6 DPA 2000.

	Storage period: There are several storage periods in different legal acts. The specific storage period for ELGA EHR-Health Data as well as electronic references) is, however, ten years (see § 20/3 EHRA 2012) for documents, one year for medication data and three years for log data.
Data integrity:	Are any specific methods used to ensure the integrity of the data? How are patients identified in the EHR? In the context of research, are anonymisation methods used and what safeguards exist for re-identification?
	Integrity of data: All HCPs are obliged by law to implement and document data security measures (see § 8/1 EHRA 2012). A specific Information Security Management System (ISMS) based on ISO directive 27000 has already been developed and is currently being implemented by the EHR-HCPs. Patient Identification: One of the central components which were created specifically for ELGA is the *Patients' Index* which aims at providing for a safe and unambiguous identification of patients. Patients are identified by way of digital certificates (usage of the citizen card [*Bürgerkarte*], a function also available as a mobile phone signature) and the Patient Index which for its part is supplied by the Central Register of Residents. Anonymisation methods in the research context: According to § 14/2 EHRA 2012, EHR-health data which are made accessible by EHR may be used in a personally identifiable manner exclusively for the purposes listed therein. The EHRA 2012 does neither list the use of medical data in the context of research, nor does it specify anonymisation methods.
Data security:	Where are the records stored? Is there a centralised database of EHR? What security technology is being used?
	Storage of records – database of EHR: EHR-health data are stored in a decentralized manner in repositories of large hospital organisations or data centers of the privates sector (so called "Affinity Domains"). Generally speaking, the ELGA "IT-Architecture" stipulates a geographically distributed system based on both centralized (shared) and decentralized patterns and components. The central components are the Patient Index, the Health Service Provider Index, the Access Control System as well as the logging and protocol feature. The only centralized EHR-healthdata base will be the information system on prescribed and dispensed medication (so called "e-Medication"). Security technology: The IT Architecture of ELGA has to comply with the EHRA 2012, the DPA 2000 and the relevant profiles of the "Integrating the Healthcare Enterprise" (IHE) standards. A specific Information Security Management System (ISMS) for the decentralized data storage has already been developed based on ISO directive 27000 and is currently being implemented by the EHR-HCPs.
Rights of the person/patient concerned:	How can the right of access be exercised? How can the data be corrected? Can the person enter information in his or her own EHR? What are the legal remedies available?
	Patients have the right to access their own health data according to Art. 19 of the Austrian Patients Charta. In the EHR context, they can retrieve their own EHR-health data by using an internet portal provided by the Federal Ministry of Health at www.gesundheit.gv.at. Data can only be corrected at the document

	source, i.e. the hospital or practice where they have been created and saved. A patient can retrieve his/her own medical data but neither change nor complete them. Medical documents can only be created by health service providers based on their professional responsibility. This rule will be not be changed by the introduction of EHR in Austria. Apart from that, data subjects have the right to access to their data according to § 26 DPA 2000. If access is not granted or not completely granted, a data subject can file a complaint with the Data Protection Authority.
Consent:	Is the system based on an opt-in approach? Is the principle of granular consent applied (with the possibility of preventing access to certain data?)? If yes, in which situations?
	ELGA is based on an opt-out approach (§15/2 EHRA 2012). One of the main arguments in favor of the opt-out rather than the opt-in approach is the lower access barrier to the e-health infrastructure provided by ELGA: Patients do not need to take any action in order to make use of ELGA and its benefits. The concept of granular consent applies in reverse insofar, as data subjects are entitled to set individual access rights for EHR-HSPs and to hide, display and delete electronic references to EHR-health data. Patients can exercise their rights at any time by means of the ELGA internet portal Furthermore, they are entitled to object the inclusion of references and EHR-Health Data including individual medication data for a concrete treatment (unless prohibited by other statutory documentation requirements) in relation to their treating or supervising EHR-HCPs (§ 16/2/2).
Withdrawal:	Are patients able to withdraw the consent given to EHR schemes? If yes, what is the relevant procedure to withdraw such consent? What are the consequences?
	As for the procedure, see above. It is important to note that the system is based on an opt-out approach. The opt-out can be declared via internet portal or paper based via opt out office (“Widerspruchstelle”) Opt-out: Patients can declare (either electronically by way of the e-Health Access Point or in writing to Opt-out Offices) their objection to the storage of their EHR-Health Data. In the case of a general objection, all data stored in the EHR are deleted. Furthermore, patients can declare their objection in each individual case to their healthcare provider.
Outsourcing processing of data:	Is outsourcing common? Under what circumstances? Where is the data outsourced to? What sort of safeguards are in place?
	The EHRA 2012 stipulates that storage media have to be based in the territory of the European Union. Outsourcing happens within the autonomy and responsibility of the health service providers. There are no notification obligations or similar for private controllers. Public controllers must in principle consult the Data Protection Authority before outsourcing sensitive data (§ 10 DPA 2000). Thus, information on the outsourcing situation is limited. The operators to whom these data are outsorced are subject to the same EHR-security requirements as healthcare providers.

2. Cloud Computing, Data Mining and Profiling from both Medical Records (including EHR) and Data not specifically related to medical records.

2.1. Data Protection Issues:

Cloud computing has brought a new dimension to the way data is stored, accessed and processed. Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS), Network as a service (NaaS) are all used by services and organisations that deal with both medical data and non-medical data.

With the development of more advanced and efficient data-mining and data-querying Medical techniques (e.g NoSQL, MapReduce, Hadoop) in conjunction with increased processing power and data storage, mining data has never been more informative, easier, and cost-effective.

Healthcare is a natural sector in which to apply new technologies and methodologies, with particular impacts in epidemiology, public health, health services research, etc.

Data that can lead to the identification of a particular individual and his/her health situation is not limited to medical data *per se,* present on Electronic Health Records, but also to unsuspicious type of information.

There is a growing concern that these schemes may be implemented in manner which does not always respect the patients' confidentiality and basic rights, and in a broader context, the use of this of information may prejudice the individuals concerned.

The ability to track and monitor patients and resources enables a more efficient provision of care but may have an impact on the right to privacy of the individual concerned.

2.2. Questions: Is your legal framework providing for a regulation of Cloud Computing, Data Mining and Profiling? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	Liability issues have to be treated by using the existing civil and data protection law. For details see http://infolaw.at/files/4_Osterreichischer_IT-Rechtstag/Blaha.pdf (in German)
Case-law:	See above
Other:	See above

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Cloud computing:	How is cloud computing regulated in your country? Which security safeguards and standards are mandatory? Are there specific requirements in order to store medical data in the cloud? How is data shared and is the sharing regulated?
	§ 6/3 EHRA 2012 stipulates that health data which are saved by means of cloud computing have to be encrypted state-of-the-art (i.e. by using protocols and methods which provide full encryption and whose cryptographic algorithms are enlisted in an ordinance issued by the Minister of Health.) The provisions of the DPA 2000 concerning data security measures (§ 14 DPA 2000) apply.
Government:	Do governmental programmes exist to allow for increased data-mining of medical records? If yes, what are the purposes of this data mining? Are private entities allowed to access the data? Under what circumstances? What sort of techniques and technologies are being used? To what end? Are data subjects informed of this type of data-mining?

	Due to the federal structure of the Republic of Austria, there is a vast amount of different ICT projects both on federal as well as on provincial and regional level. For an overview over the projects on federal level see www.iktprojekte.at. This overview does not contain any data mining projects. The Austrian social security institutions are granted autonomy and special data procession rights based on the Social Security Act. Data mining is, however not explicitly mentioned.
Private sector:	Are private entities allowed to mine medical data which they process? Under what circumstances? Can the government have access to this data?
	Anyone willing to carry out data mining must comply with the DPA 2000. The DPA 2000 contains a special provision on the use of data for research purposes in § 46. In certain cases an approval of the Data Protection Authority is required. For further information and findings of scientific research see http://rechtsinformatik.univie.ac.at/forschung/
Profiling:	Are the government and the private sector allowed to employ profiling methods on medical data? If yes, under what circumstances? Is it allowed to cross and correlate non-medical data with medical data?
	See above.

3. RFID and wireless communication technologies

3.1. Data Protection Issues:

It is common for medical devices, such as patients' tags, to possess RFID technologies in order to facilitate the transmission of the patients' data.

It can also be related to the data-mining operations previously mentioned as it is another category of information that can be used to discern meaningful patterns.

Transmission of data through radio-frequency is not limited to medical devices. Almost any smartphone uses some technology enabling to collect, and share, the user's data. For instance, via WI-FI it is possible to identify users' locations and therefore infer some of their behaviour, which in some cases can relate to health information.

3.2. Questions: Is your legal framework providing for a regulation of RFID technologies and the transfer of personal data through wireless technologies? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	The general provisions of the DPA 2000 apply.
Case-law:	No case-law
Other:	----------

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
RFID:	How is RFID used in hospital/clinics for (a) resource management, (b) patient care? What types of database systems (and security) are implemented in conjunction with RFID use? How are issues of access, sharing, consent etc.

	managed considering that RFID may be used without the patients' knowledge.
	Identification of medical devices is organized by using the bar code system of Global Standard One. See http://www.gs1.at/branchenloesungen/gesundheitswesen/gs1-anwendungen In this context, RFID is also applied in individual hospitals. See http://www.aerztezeitung.at/archiv/oeaez-2009/oeaez-7-10042009/13-internationale-gs1-healthcare-konferenz-krankenhaus-der-zukunft.html
Wireless tracking technologies:	Are hospitals/clinics employing other wireless tracking technologies besides RFID? Which ones? Do they have to follow specific security requirements? Which ones?
	----------

4. Applications (Mobile)

4.1. Data Protection Issues:

Information society is increasingly relying on the use of "apps" (application), most of them mobile. These apps are commonly designed to gather personal data, and in practice often process medical data.
Technologies such as multi-touch touchscreen, accelerometers or gyroscopes, ambient light sensors, GPS and cameras, and devices featuring fingerprint and biometric sensors also involve the collection of medical data.

A mobile phone application can monitor accurately physiological data, such as heartbeats, sleep patterns, fitness information.

4.2. Questions: Is your legal framework providing for a regulation of Apps and Mobile Apps? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	There is no specific legislation for a regulation of Apps and Mobile Apps; the general provisions of the DPA 2000 apply.
Case-law:	No case-law
Other:	----------

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Apps:	Is it allowed to use apps and mobile apps to deploy medical services and collect medical data? If yes, which type of individual/organisation can develop and employ these apps? Are there specific security requirements for these types of apps?

Institutions:	Do hospitals/clinics/labs employ apps to gather medical data? Is there a need for a medical treatment to permit the use of an app to process the medical data? Are there specific security requirements for the institutions collecting these data from the apps? Are medico-administrative data used by hospitals/clinics for management purposes?

Tracking	Do hospitals/clinics/labs employ non-medical apps and devices to track and collect

technologies:	data from their patients? What type of data is collected? For what purpose? Is the data identifiable? Is the data combined with medical data?

Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical apps and tracking apps? If yes, what are the standards?

Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical diagnostic? How would this be applied to fitness and daily-basis data?
	---

5. Medical Devices and Wearable Devices

5.1. Data Protection Issues:

A medical device can be defined as: 'any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application. Such a device should be intended by the manufacturer for one of a number of defined purposes, one of which is, diagnosis, prevention, monitoring, treatment or alleviation of disease' (Directive 93/42/EEC Article 1:2)

Some eHealth and mHealth devices and apps do not fall in this definition of medical devices, as can also be the case of a software working in combination with a physical device, for instance a smartphone.

5.2. Questions: Is your legal framework providing for a regulation of Medical Devices? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	Yes, medical devices are regulated by the "Federal Act on Medical Devices (Medizinproduktegesetz – MPG)", available (in German) online at www.ris.bka.gv.at/GeltendeFassung/Bundesnormen/10011003/MPG%2c%20Fassung%20vom%2029.10.2014.pdf
Case-law:	No case-law
Other:	----------

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
eHealth and mHealth:	Does the concept of Medical device in your country encompass services and apparels in the realm of eHealth and mHealth? What are the requirements? Should, for instance, the medical device be certified before it can be used?
	No. A certification is required only under the Federal Act on Medical Devices.
Apps:	Does the concept of medical devices encompass apps? If yes, is there any regulation applicable to apps that perform medical services? Is there any regulation applicable on apps that track non-medical data that can lead to health information? If yes, what type of data?

	No
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical and/or wearable devices? If yes, what are the standards?
	No specific requirement; the DPA 2000 stipulates the general applicable data minimization principle.
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical treatment? How would this be applied to fitness and daily-basis data?
	----------

6. Internet of Things

6.1. Data Protection Issues:

Internet of things relates to common, ordinary devices that are now, and increasingly, connected to the Internet, such as cars, fridges, ovens, microwaves, etc. All of these devices can provide data that can lead to reveal information concerning one's health. A fridge can easily inform on the type of food stored and thus the diet of an individual. One of the biggest challenges of the Internet of Things is to guarantee the right to privacy and data protection in a world where every device collects, processes, analyses and transmits the data, commonly via wireless technologies.

In the realm of medical data, the issue mainly arises when crossing seemly unrelated data that can lead to health information about an individual.

6.2. Questions: Is your legal framework providing for a regulation of the Internet of Things? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	For the government strategies concerning digital services see http://www.digitales.oesterreich.gv.at/. "Internet of Things" is not mentioned. There is no specific legal framework; the general provisions of the DPA 2000 apply.
Case-law:	See above
Other:	See above

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Security:	What are the security standards that need to be employed by these devices when collecting personal data?
	See above
Non-medical devices:	Are non-medical devices allowed to collect medical data, such as heart frequency? Are they allowed to cross medical data with non-medical data?
	See above
Privacy by Design:	Is there any requirement to implement privacy by design in the development of connected devices? If yes, what are the standards?

	See above

7. Electronic Doctor (online Doctor) and on-line appointments

7.1. Data Protection Issues:

The Doctor listens, talks and assesses the patient online, via a website, app, canal, sometimes including video-conference. Medical data is collected and processed, what are the security requirements and standards followed? Other websites provide for on-line appointments with doctors, which can also involve the processing of medical data.

7.2. Questions: Is your legal framework providing for a regulation of online Medical Treatment and is the on-line appointment system covered by such a framework? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	According to § 49/2 Ärztegesetz, medical doctors are obliged to carry out their professional duties personally and directly. Thus online medical treatment is unlawful in Austria.
Case-law:	----------
Other:	----------

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Medical treatment:	Is it allowed to perform medical treatment via online services? If yes, how should the medical services be provided? Does it have to follow the same requirements of a regular physically-present medical treatment?
	See above
Medical data:	How should the data collected via a medical treatment performed online be processed? Are there specific requirements? Which ones?
	See above

Other comments and technologies
Should you wish to describe any technology, feature or trend that has not been covered by the questionnaire, please feel free to use the space provided below. Where relevant, also indicate recent legislation changes, guidelines and/or case law.

BELGIUM / BELGIQUE

QUESTIONNAIRE

The questionnaire should ideally be completed by data protection authorities, health policy authorities, professional or patient associations as well as healthcare providers: you are invited to share it as widely as possible.

Please send your replies to dataprotection@coe.int no later than 15 December 2014.

1. Mobile Health (mHealth) and Electronic Health Records (EHR)

1.1. Data Protection Issues:

This is perhaps the biggest topic sitting at the intersection of technology and data protection. Mobile health (mHealth) and Electronic Health Records (EHR) are increasingly used in healthcare systems and provisions – it is a trend that needs to be examined.

Related to the EHR, these records are more accurate, cost-effective (in terms of storage) than paper-based notes. The concept of patient controlled/accessed EHR has been implemented in varying degrees in different countries.

Furthermore, some non-medical record can still contain health information about users and it should be considered if such records ought to be treated in a similar way to EHR.

Also, should 'medical data' as defined in Recommendation N° (97) 5 on the protection of medical data cover physical tracking data, such as pedometers or fitness data and data that can lead to medical information about an individual ?

1.2. Questions: if EHR exist in your country, is your legal framework providing for a regulation of such records? If mHealth exists in your country, is your legal framework providing for a specific regulation? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	The general data protection legislation (the Belgian law on data protection of December 8th of 1992) applies to all health records, both to those held on paper as to those held electronically. Nevertheless, the Belgian law of August 21st of 2008 *concerning the establishment and organization of the eHealth-platform* aims to facilitate the exchange of electronic health data/records that are stored in a decentralized way: a directory of referral indicates where health data of a certain person/patient is held/stored and can be found (e.g., which hospital). The legislation also provides for certain services ensuring for a secure transmission of sensitive health data (encryption, encoding, time stamping, loggings, etc …)
Case-law:	/
Other:	The Belgian DPA did render an opinion on the aforementioned bill *concerning the establishment and organization of the eHealth-platform* (Opinion n° 14/2008 of April 2nd 2008). In this opinion the Belgian DPA highlighted (a.o.) the obligation to comply with the general privacy legislation (the Belgian law on data protection) and the Belgian legislation on patient rights, and more in particular with the right of each patient to know at all times who accessed his personal data and at what time.

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines,

DPAs' opinions and/or case law).	
EHR and Medical data:	What can be considered medical data in your country? Is it solely the data relating to a person's health (state, diagnosis, prognosis, medical treatment, etc.)? Is non-medical data that leads to medical information treated the same way as medical data (for instance in terms of confidentiality requirements)? Is the EHR solely constituted of data collected in a medical context or can the individual also himself or herself add information regarding his or her health?
	Medical data are data that contain information about the health status of an individual. Even though the Belgian law on data protection doesn't provide in a definition of 'personal data concerning health', for the Belgian DPA this refers to: all information concerning the past, present and future, physical or mental health of an individual. This implies that, when the use of 'non-medical data by nature' leads to medical information, this data will be treated the same way as 'medical data by nature'. Privacy legislation only uses 'data concerning the health status of an individual'. No distinction is made with respect to the context in which the data is gathered (non-medical or medical context). In Belgium, health professionals are responsible for the content of an EHR and the data are traditionally obtained in a medical context. According to patient rights' legislation a patient can ask the health professional to add certain documents to his health record. However and recently, efforts are being made for the development of a Personal Health Record (PHR) in which a patient can view (a summary of) his or her own medical data stored in the EHR of a medical doctor. A PHR should also allow the patient to store and share self-generated medical data.
Sharing of data and Access:	Who is granted access to the EHR and how is the sharing of information (with other health care providers?) regulated? Where information is shared with pharmacists, is there a strict purpose limitation in place? How has the definition of the responsibility over the medical data been regulated?
	Typically only the treating physicians or health professionals have access to the data in an EHR. However, patient's rights legislation gives a patient the right to view his or her own medical data and to obtain a copy of the medical record. Recently and as stated above, efforts are being made to give patients direct access to their own electronic information through the PHR. Sharing of digital health care data is possible through the standards and (basic) services of the Belgian eHealth-platform (https://www.ehealth.fgov.be/nl/home) and the services with added value that use the functionality of the eHealth-platform (e.g., Vitalink in Flanders (www.vitalink.be), Intermed in Wallonia – which are health vaults for specific health information like the medication or vaccination scheme or a summary electronic health record – or the Hubs & Metahub system). Any other exchange of health-related personal data (outside the scope of the therapeutic relationship between patients and healthcare professionals and outside any regulatory requirement) has to be authorized by the Sector Committee of Social Security and Health (established within the Belgian Privacy Commission), prior to the exchange. This committee will examine the lawfulness, legitimacy, proportionality and security of the exchange/communication of health-related personal data.

	Sharing of health data between health professionals through the eHealth-platform is also subject to an informed consent of the patient (electronic opt-in procedure available on the website of the eHealth-platform). Data exchange with pharmacists is only on a need to know basis. There is no single responsible for medical data. A health professional is responsible for the data that he/she generates for his/her own patients. He can be considered as 'controller' of his patient records. In larger organizations, the one that determines the purposes and means of the processing or the one designated as such by law, will be considered as controller, and therefore responsible for the processing of the data, assisted in this by security consultants, the data protection officer and/or the Chief Medical Officer. The Belgian data protection legislation dictates that health-related personal data may only be processed under the responsibility of a health-care professional. The controller will therefore appoint such a health-care professional to take this responsibility.
Data quality:	Are the principles of legitimacy, fairness and minimisation applied to medical data? How are records kept accurate? How long is the data kept for, is the specific storage period defined for the EHR?
	All data protection principles are applied to health-related personal data. Health professionals are responsible for the accuracy of the data in their field of expertise that they generate in their own medical records for their own patients. General practitioners can receive a fee to gather and centralize all the relevant medical information from every treating physician for a certain patient (Global medical record). Medical records have to be kept for 30 years after that last contact with the patient; regardless electronic storage or on paper.
Data integrity:	Are any specific methods used to ensure the integrity of the data? How are patients identified in the EHR? In the context of research, are anonymisation methods used and what safeguards exist for re-identification?
	The Belgian eHealth-platform offers certain services to ensure integrity of the data, such as time stamping. Patients are identified through their Identification Number of Social Security, which for most Belgian citizens is identical to their Identification Number of the National Registry. Belgian data protection legislation dictates that (further) processing for research purposes should preferably be realized by using anonymous data; when the research purpose cannot be achieved using anonymous data, encoded data may be processed. Only when the use of encoded data doesn't allow to achieve the research purpose, non-encoded data can be used. The eHealth-platform can act as a Trusted Third Party (TTP) for anonymisation or coding of patient data.
Data security:	Where are the records stored? Is there a centralised database of EHR? What security technology is being used?
	Data storage is typically decentralized. Every hospital usually has his own local system. The same applies to general practitioners who have GP-oriented packages to their disposal with data storage that is usually local. (up until April 2014 hospitals were even legally obliged to store their medical records 'in house' – cloud computing was therefore not feasible) Recently,

	GP-oriented EHR-systems became available that are cloud-based. Data however, cannot be accessed by colleagues that are not directly associated with the treating physician. In Flanders Vitalink (www.vitalink.be) serves as a central health database designed to share specifically selected health information (see above) between different health professions and between health professionals and patients. A similar system exists in Wallonia (Intermed). Regardless the way personal data are processed or stored, certain security measures should always be implemented. The Belgian DPA listed the following reference measures: information security policy, organization of information security, physical environment security, network security, logical access security, access logging (audit trails and access analysis), monitoring – checks – maintenance, security incident management and continuity, enforcement, documentation (for more detailed information: http://www.privacycommission.be/sites/privacycommission/files/documents/reference_measures_security_personal_data_processing_1.pdf)
Rights of the person/patient concerned:	How can the right of access be exercised? How can the data be corrected? Can the person enter information in his or her own EHR? What are the legal remedies available?
	The right of access is provided for by the general data protection legislation and by the patient's rights legislation. Every patient has the right of access (directly of by means/intervention of a healthcare professional) to his medical record. A patient can also request for a copy of his patient file. At this moment, a patient cannot enter himself, any information into his health record directly; he can, however, ask the health care professional to add certain documents or information. The development of a PHR should allow the patient to do this independently. General data protection legislation allows any person to rectify incorrect personal data relating to him. Data protection legislation imposes a fine on any controller who fails to answer a right of access within forty-five days of receipt of the request. According to patient's rights legislation a patient can introduce a complaint regarding the exercise of his rights in the hands of the competent Ombudsman.
Consent:	Is the system based on an opt-in approach? Is the principle of granular consent applied (with the possibility of preventing access to certain data?)? If yes, in which situations?
	Sharing of health data between health professionals through the eHealth-platform is subject to an informed consent of the patient (electronic opt-in procedure available on the website of the eHealth-platform). Physicians can be included or excluded. No granular consent is possible for certain categories of data.
Withdrawal:	Are patients able to withdraw the consent given to EHR schemes? If yes, what is the relevant procedure to withdraw such consent? What are the consequences?
	Opt-in (see above) for data sharing through the eHealth-platform can be withdrawn immediately and at any time on the website of the eHealth-platform. On the level of hospitals or individual physicians, no such opt-in or opt-out procedure exists. Processing of health data by individual hospitals or healthcare professionals is, indeed, not based on 'consent' but on the necessity of this processing within the scope of preventive medicine or medical diagnosis, the provision of care or treatment or the management of healthcare services.
Outsourci	Is outsourcing common? Under what circumstances? Where is the data outsourced to? What

ng processing of data:	sort of safeguards are in place? Outsourcing is not common.

2. Cloud Computing, Data Mining and Profiling from both Medical Records (including EHR) and Data not specifically related to medical records.

2.1. Data Protection Issues:

Cloud computing has brought a new dimension to the way data is stored, accessed and processed. Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS), Network as a service (NaaS) are all used by services and organisations that deal with both medical data and non-medical data.

With the development of more advanced and efficient data-mining and data-querying Medical techniques (e.g NoSQL, MapReduce, Hadoop) in conjunction with increased processing power and data storage, mining data has never been more informative, easier, and cost-effective.

Healthcare is a natural sector in which to apply new technologies and methodologies, with particular impacts in epidemiology, public health, health services research, etc.

Data that can lead to the identification of a particular individual and his/her health situation is not limited to medical data *per se,* present on Electronic Health Records, but also to unsuspicious type of information.

There is a growing concern that these schemes may be implemented in manner which does not always respect the patients' confidentiality and basic rights, and in a broader context, the use of this of information may prejudice the individuals concerned.

The ability to track and monitor patients and resources enables a more efficient provision of care but may have an impact on the right to privacy of the individual concerned.

2.2. Questions: Is your legal framework providing for a regulation of Cloud Computing, Data Mining and Profiling? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	The Belgian legal framework does not provide in any specific regulation concerning cloud computing, data mining or profiling. General data protection legislation and principles apply.
Case-law:	/
Other:	The Belgian DPA did not yet render any opinions, guidelines, recommendations, … concerning cloud computing, data mining or profiling.

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Cloud computing:	How is cloud computing regulated in your country? Which security safeguards and standards are mandatory? Are there specific requirements in order to store medical data in the cloud? How is data shared and is the sharing regulated?

	As stated above, no specific regulation concerning the use of cloud computing with regard to the processing of health-related data exists in Belgium. Up until April 2014 cloud computing was not even an option for hospitals, since hospitals were obliged to hold/store their medical records 'in house'. At the moment a circular letter with guidelines regarding the use of cloud based systems in hospitals, is being prepared by the ministry of social affairs and public health.
Government:	Do governmental programmes exist to allow for increased data-mining of medical records? If yes, what are the purposes of this data mining? Are private entities allowed to access the data? Under what circumstances? What sort of techniques and technologies are being used? To what end? Are data subjects informed of this type of data-mining?
	No
Private sector:	Are private entities allowed to mine medical data which they process? Under what circumstances? Can the government have access to this data?
	Yes under certain circumstances. For as far general data protection principles applied to health-related personal data (purpose limitation in particular) are respected this may be allowed.
Profiling:	Are the government and the private sector allowed to employ profiling methods on medical data? If yes, under what circumstances? Is it allowed to cross and correlate non-medical data with medical data?
	Secondary use and further processing can be allowed when not incompatible with the initial purpose of processing and when respecting all other data protection principles (applied to the processing of health-related personal data). Nevertheless, any communication (crossing and correlation implied) of health-related personal data (outside the scope of the therapeutical relation between patient and healthcare professional and outside any regulatory requirement) is only possible after prior authorization from the Belgian Sector Committee of Social Security and Health (see before).

3. RFID and wireless communication technologies

3.1. Data Protection Issues:

It is common for medical devices, such as patients' tags, to possess RFID technologies in order to facilitate the transmission of the patients' data.

It can also be related to the data-mining operations previously mentioned as it is another category of information that can be used to discern meaningful patterns.

Transmission of data through radio-frequency is not limited to medical devices. Almost any smartphone uses some technology enabling to collect, and share, the user's data. For instance, via WI-FI it is possible to identify users' locations and therefore infer some of their behaviour, which in some cases can relate to health information.

3.2. Questions: Is your legal framework providing for a regulation of RFID technologies and the transfer of personal data through wireless technologies? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	The Belgian legal framework does not provide in any specific regulation concerning RFID technologies. General data protection legislation and principles apply.
Case-law:	/
Other:	The Belgian DPA did render an opinion on the use of RFID in general (Opinion n°27/2009 of October 14th 2009) in which she draw the attention (a.o.) on: a freely given and informed consent by the data subject, the necessity of a privacy impact assessment and efficient technical and organizational security measures that comply with technological evolution and developments.

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
RFID:	How is RFID used in hospital/clinics for (a) resource management, (b) patient care? What types of database systems (and security) are implemented in conjunction with RFID use? How are issues of access, sharing, consent etc. managed considering that RFID may be used without the patients' knowledge.
	RFID technology is used in some hospitals for patient identification mainly to prevent erroneous patient switch. In some cases, it is also used during equipment sterilization procedures (quality control) and for logistic purposes.
Wireless tracking technologies:	Are hospitals/clinics employing other wireless tracking technologies besides RFID? Which ones? Do they have to follow specific security requirements? Which ones?

4. Applications (Mobile)

4.1. Data Protection Issues:

Information society is increasingly relying on the use of "apps" (application), most of them mobile. These apps are commonly designed to gather personal data, and in practice often process medical data.
Technologies such as multi-touch touchscreen, accelerometers or gyroscopes, ambient light sensors, GPS and cameras, and devices featuring fingerprint and biometric sensors also involve the collection of medical data.

A mobile phone application can monitor accurately physiological data, such as heartbeats, sleep patterns, fitness information.

4.2. Questions: Is your legal framework providing for a regulation of Apps and Mobile Apps? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	The Belgian legal framework does not provide in any specific regulation concerning Apps and Mobile Apps. General data protection legislation and principles apply.
Case-law:	/

Other:	The Belgian DPA did not yet render any opinions, guidelines, recommendations, … concerning Apps and Mobile Apps.

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Apps:	Is it allowed to use apps and mobile apps to deploy medical services and collect medical data? If yes, which type of individual/organisation can develop and employ these apps? Are there specific security requirements for these types of apps?
	Yes. As stated above, no specific regulation concerning the use of Apps and Mobile Apps with regard to the processing of health-related data exists in Belgium. General privacy legislation applies. In principle, the basic services and standards of the eHealth-platform could be used to communicate health data.
Institutions:	Do hospitals/clinics/labs employ apps to gather medical data? Is there a need for a medical treatment to permit the use of an app to process the medical data? Are there specific security requirements for the institutions collecting these data from the apps? Are medico-administrative data used by hospitals/clinics for management purposes?
	At this moment, we do not know any specific examples of hospitals that use smartphone apps to gather medical data (e.g., for telemonitoring – also see Section Other comments and technologies) but in principle this could be possible in the context of a medical evaluation or treatment. The general privacy legislation applies. Note that there some software firms of EHR software for GP's have mobile versions of their applications. Hospitals use medico-administrative data to optimize their revenues, services, internal procedures and policies.
Tracking technologies:	Do hospitals/clinics/labs employ non-medical apps and devices to track and collect data from their patients? What type of data is collected? For what purpose? Is the data identifiable? Is the data combined with medical data?
	Not to our knowledge.
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical apps and tracking apps? If yes, what are the standards?
	Not to our knowledge.
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical diagnostic? How would this be applied to fitness and daily-basis data?
	It should be based on an opt-in approach. No regulation exists stating that the data collection should be in reference to a specific medical diagnostic.

5. Medical Devices and Wearable Devices

5.1. Data Protection Issues:
A medical device can be defined as: 'any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application. Such a device should be intended by the manufacturer for one of a number of defined purposes, one of which is, diagnosis, prevention, monitoring, treatment or alleviation of disease' (Directive 93/42/EEC Article 1:2) Some eHealth and mHealth devices and apps do not fall in this definition of medical devices, as can also be the case of a software working in combination with a physical device, for instance a smartphone.

5.2. Questions: Is your legal framework providing for a regulation of Medical Devices? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	The Royale Decree of March 18th of 1999 *concerning medical devices* (see below) The law of December 2013 15th *concerning medical devices*
Case-law:	/
Other:	Regardless some -mostly formal- remarks, the Belgian DPA did render a favorable opinion on the aforementioned bill *concerning medical devices* (Opinion n° 34/2013 of July 17th 2013).

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
eHealth and mHealth:	Does the concept of Medical device in your country encompass services and apparels in the realm of eHealth and mHealth? What are the requirements? Should, for instance, the medical device be certified before it can be used?
	The royal decree on medical devices in Belgium (18/03/1999) is based on the European directive on medical devices (1993/42) which states: 'Medical device' means any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application, intended by the manufacturer to be used for human beings for the purpose of: — diagnosis, prevention, monitoring, treatment or alleviation of disease, — diagnosis, monitoring, treatment, alleviation of or compensation for an injury or handicap, — investigation, replacement or modification of the anatomy or of a physiological process, — control of conception, and which does not achieve its principal intended action in or on the human body by pharmacological, immunological or metabolic means, but which may be assisted in its function by such means; In our opinion, this can encompass the above-mentioned services and apparels in the realm of eHealth and mHealth.

	A CE-label should be obtained before introduction to the market is allowed. Recognition is necessary with the Federal Agency for Medicines and HealthProducts and all incidents must be notified. The FAMHP is the Belgian competent authority responsible for quality, safety and efficacy of pharmaceutical and health products from development to application (http://www.fagg-afmps.be/en/). Although not yet in effect, article 51 of the aforementioned law of December 13th 2013 foresees the installation of a central registry within the FAMHP for all implants in order to make sure they remain traceable.
Apps:	Does the concept of medical devices encompass apps? If yes, is there any regulation applicable to apps that perform medical services? Is there any regulation applicable on apps that track non-medical data that can lead to health information? If yes, what type of data?
	In principle the above-mentioned definition of medical devices encompasses health apps. See above for the regulatory requirements. The general data protection legislation and principles apply.
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical and/or wearable devices? If yes, what are the standards?
	Not to our knowledge. The general data protection legislation and principles apply.
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical treatment? How would this be applied to fitness and daily-basis data?
	It should be based on an opt-in approach. The general data protection legislation applies. No regulation exists stating that the data collection should be in reference to a specific medical treatment and we think that this is not always warranted or desired (e.g., devices for prevention or in the wellness domain).

6. Internet of Things

6.1. Data Protection Issues:

Internet of things relates to common, ordinary devices that are now, and increasingly, connected to the Internet, such as cars, fridges, ovens, microwaves, etc. All of these devices can provide data that can lead to reveal information concerning one's health. A fridge can easily inform on the type of food stored and thus the diet of an individual. One of the biggest challenges of the Internet of Things is to guarantee the right to privacy and data protection in a world where every device collects, processes, analyses and transmits the data, commonly via wireless technologies.

In the realm of medical data, the issue mainly arises when crossing seemly unrelated data that can lead to health information about an individual.

6.2. Questions: Is your legal framework providing for a regulation of the Internet of Things? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	The Belgian legal framework does not provide in any specific regulation concerning the Internet of Things. General data protection legislation and principles apply.
Case-law:	/
Other:	The Belgian DPA did not yet render any opinions, guidelines, recommendations, … concerning the Internet of Things.

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Security:	What are the security standards that need to be employed by these devices when collecting personal data?
	As stated above, no specific regulation concerning these devices with regard to the processing of health-related data exists in Belgium. General privacy legislation applies.
Non-medical devices:	Are non-medical devices allowed to collect medical data, such as heart frequency? Are they allowed to cross medical data with non-medical data?
	General privacy legislation concerning health data applies. Any communication (crossing implied) of health-related personal data -outside the scope of the therapeutical relation between patient and health care professional and outside any regulatory requirement- is only possible after prior authorization from the Belgian Sector Committee of Social Security and Health (see before).
Privacy by Design:	Is there any requirement to implement privacy by design in the development of connected devices? If yes, what are the standards?
	Not to our knowledge.

7. Electronic Doctor (online Doctor) and on-line appointments

7.1. Data Protection Issues:

The Doctor listens, talks and assesses the patient online, via a website, app, canal, sometimes including video-conference. Medical data is collected and processed, what are the security requirements and standards followed? Other websites provide for on-line appointments with doctors, which can also involve the processing of medical data.

7.2. Questions: Is your legal framework providing for a regulation of online Medical Treatment and is the on-line appointment system covered by such a framework? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	The Belgian legal framework does not provide in any specific regulation concerning online Medical Treatment. General data protection legislation and principles apply.
Case-law:	/
Other:	The Belgian DPA did not yet render any opinions, guidelines, recommendations, … concerning online Medical Treatment.

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Medical treatment:	Is it allowed to perform medical treatment via online services? If yes, how should the medical services be provided? Does it have to follow the same requirements of a regular physically-present medical treatment?
	At this moment, medical deontology in Belgium requires that a physician is physically present during a consultation with a patient (because a medical evaluation almost always requires one or another form of clinical examination which is not possible through online services).
Medical data:	How should the data collected via a medical treatment performed online be processed? Are there specific requirements? Which ones?
	General privacy legislation concerning health data applies but as stated above and in principle, physicians should be reluctant to participate in online treatment or diagnosis.

Other comments and technologies
Should you wish to describe any technology, feature or trend that has not been covered by the questionnaire, please feel free to use the space provided below. Where relevant, also indicate recent legislation changes, guidelines and/or case law.
Hospitals and hospital physician participate more and more in telemonitoring projects where several parameters (dependent on the specific health problem; e.g., for COPD, heart failure or arrhythmias) are measured at home - usually with specific and dedicated hardware and software (not necessarily apps but this could be possible), stored (locally and/or in a remote database), transmitted (sometimes in real time) and interpreted automatically and/or manually. No specific legislation has yet been developed, but the general privacy legislation applies.

BOSNIA AND HERZEGOVINA

QUESTIONNAIRE

The questionnaire should ideally be completed by data protection authorities, health policy authorities, professional or patient associations as well as healthcare providers: you are invited to share it as widely as possible.

Please send your replies to dataprotection@coe.int no later than 15 December 2014.

1. Mobile Health (mHealth) and Electronic Health Records (EHR)

1.1. Data Protection Issues:

This is perhaps the biggest topic sitting at the intersection of technology and data protection. Mobile health (mHealth) and Electronic Health Records (EHR) are increasingly used in healthcare systems and provisions – it is a trend that needs to be examined.

Related to the EHR, these records are more accurate, cost-effective (in terms of storage) than paper-based notes. The concept of patient controlled/accessed EHR has been implemented in varying degrees in different countries.

Furthermore, some non-medical record can still contain health information about users and it should be considered if such records ought to be treated in a similar way to EHR.

Also, should 'medical data' as defined in Recommendation N° (97) 5 on the protection of medical data cover physical tracking data, such as pedometers or fitness data and data that can lead to medical information about an individual ?

1.2. Questions: if EHR exist in your country, is your legal framework providing for a regulation of such records? If mHealth exists in your country, is your legal framework providing for a specific regulation? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	EHR in BIH is currently being established and it is used in some medical institutions. At the entity level (FBiH and RS) the Law on Health Record in the Health Field of Federation of BiH ("Off. Gazette of FBiH" No.37/12) and the Law on Records and Statistical Researches in the Health Field of the Republic of Srpska ("Official Gazette of RS" No. 53/07) were adopted, prescribing the records in the health field, keeping methods, etc. Relevant regulations that generally relate to health care are: The Law on Health Protection of RS ("Official Gazette" No. 106/09) The Law on Health Protection of FBiH ("Official Gazette" of FBiH" No.46/10 and 75/13) The Law on the Rights, Obligations and Responsibilities of patients in FBiH ("Official Gazette of BiH" No.40/10) These laws stipulate fines as a kind of sanctions for violators of the provisions thereof.
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
EHR and Medical data:	What can be considered medical data in your country? Is it solely the data relating to a person's health (state, diagnosis, prognosis, medical treatment, etc.)? Is non-medical data that leads to medical information treated the same way as medical data (for instance in terms of confidentiality requirements)? Is the EHR solely constituted of data collected in a medical context or can the individual also himself or herself add information regarding his or her health?
	Medical data are the ones that relate to health of a person and that are defined as a separate category of personal data, and in terms of the Law on Personal Data Protection, each entry, on the basis of which the medical condition can be determined or disclosed, falls into a special category of data. Health data of an individual are processed in the framework of health records (electronic or material) containing the medical documentation relating to that person. Medical documentation includes written, electronic and other evidence to support certain allegations, which were collected and secured in the process of implementing health care.
Sharing of data and Access:	Who is granted access to the EHR and how is the sharing of information (with other health care providers?) regulated? Where information is shared with pharmacists, is there a strict purpose limitation in place? How has the definition of the responsibility over the medical data been regulated?
	Only authorized doctor of medicine granted access to the EHR. EHR in BiH has currently been established only in some health institutions and the introduction of electronic prescriptions and establishing communication with pharmacies will gradually be implemented in the coming period.
Data quality:	Are the principles of legitimacy, fairness and minimisation applied to medical data? How are records kept accurate? How long is the data kept for, is the specific storage period defined for the EHR?
	The Law on Health Records in the health field of Federation of BiH ("Off. Gazette of FBiH" No.37/12) and the Law on Records and Statistical Researches in the Health Field of the Republic of Srpska ("Official Gazette of RS" No. 53/07) prescribe the basis, minimum of required data and responsibility for the accuracy of the data entered. Keeping health data is limited, only dental records are kept permanently.
Data integrity:	Are any specific methods used to ensure the integrity of the data? How are patients identified in the EHR? In the context of research, are anonymisation methods used and what safeguards exist for re-identification?
	Laws provide that secondary legislation closely defines the architecture of the health-information system.
Data security:	Where are the records stored? Is there a centralised database of EHR? What security technology is being used?
	Electronic records and EHR are stored on a separate partition on the server and they are being backed up on a server or external hard drive.
Rights of the person/patient concerned:	How can the right of access be exercised? How can the data be corrected? Can the person enter information in his or her own EHR? What are the legal remedies available?
	The patient has the right to timely information needed in order to decide whether to agree or not to a proposed medical measure. Informing the patient should be sufficiently comprehensive, accurate and timely.

	The right to access information can be achieved by each patient himself according to the Law on Personal Data Protection. Statement of the patient can be a source of data for entry into the medical documentation.
Consent:	Is the system based on an opt-in approach? Is the principle of granular consent applied (with the possibility of preventing access to certain data?)? If yes, in which situations?
	Data access can be restricted pursuant to Article 28 of the Law on Personal Data Protection because of: national security, defense, public security, health protection, prevention, investigation etc.
Withdrawal:	Are patients able to withdraw the consent given to EHR schemes? If yes, what is the relevant procedure to withdraw such consent? What are the consequences?
	Personal data subject has the right to rectification, erasure and blocking of data that are inaccurate, incorrectly stated or processed in a manner contrary to the law and rules of processing (Article 27 of the Law on Personal Data Protection).
Outsourcing processing of data:	Is outsourcing common? Under what circumstances? Where is the data outsourced to? What sort of safeguards are in place?

2. Cloud Computing, Data Mining and Profiling from both Medical Records (including EHR) and Data not specifically related to medical records.

2.1. Data Protection Issues:

Cloud computing has brought a new dimension to the way data is stored, accessed and processed. Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS), Network as a service (NaaS) are all used by services and organisations that deal with both medical data and non-medical data.

With the development of more advanced and efficient data-mining and data-querying Medical techniques (e.g NoSQL, MapReduce, Hadoop) in conjunction with increased processing power and data storage, mining data has never been more informative, easier, and cost-effective.

Healthcare is a natural sector in which to apply new technologies and methodologies, with particular impacts in epidemiology, public health, health services research, etc.

Data that can lead to the identification of a particular individual and his/her health situation is not limited to medical data *per se,* present on Electronic Health Records, but also to unsuspicious type of information.

There is a growing concern that these schemes may be implemented in manner which does not always respect the patients' confidentiality and basic rights, and in a broader context, the use of this of information may prejudice the individuals concerned.

The ability to track and monitor patients and resources enables a more efficient provision of care but may have an impact on the right to privacy of the individual concerned.

2.2. Questions: Is your legal framework providing for a regulation of Cloud Computing, Data Mining and Profiling? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs'

opinions and/or case law.	
Legislation:	No. Application of the principle of legitimate processing of personal data and specific provisions relating to the processing of special categories of personal data, and for the violation of the same, the Law provides criminal provisions.
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Cloud computing:	How is cloud computing regulated in your country? Which security safeguards and standards are mandatory? Are there specific requirements in order to store medical data in the cloud? How is data shared and is the sharing regulated?
Government:	Do governmental programmes exist to allow for increased data-mining of medical records? If yes, what are the purposes of this data mining? Are private entities allowed to access the data? Under what circumstances? What sort of techniques and technologies are being used? To what end? Are data subjects informed of this type of data-mining?
Private sector:	Are private entities allowed to mine medical data which they process? Under what circumstances? Can the government have access to this data?
Profiling:	Are the government and the private sector allowed to employ profiling methods on medical data? If yes, under what circumstances? Is it allowed to cross and correlate non-medical data with medical data?

3. RFID and wireless communication technologies

3.1. Data Protection Issues:

It is common for medical devices, such as patients' tags, to possess RFID technologies in order to facilitate the transmission of the patients' data.

It can also be related to the data-mining operations previously mentioned as it is another category of information that can be used to discern meaningful patterns.

Transmission of data through radio-frequency is not limited to medical devices. Almost any smartphone uses some technology enabling to collect, and share, the user's data. For instance, via WI-FI it is possible to identify users' locations and therefore infer some of their behaviour, which in some cases can relate to health information.

3.2. Questions: Is your legal framework providing for a regulation of RFID technologies and the transfer of personal data through wireless technologies? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	No. Application of the principle of legitimate processing of personal data and specific provisions relating to the processing of special categories of personal data, and for

	the violation of the same, the Law provides criminal provisions.
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
RFID:	How is RFID used in hospital/clinics for (a) resource management, (b) patient care? What types of database systems (and security) are implemented in conjunction with RFID use? How are issues of access, sharing, consent etc. managed considering that RFID may be used without the patients' knowledge.
Wireless tracking technologies:	Are hospitals/clinics employing other wireless tracking technologies besides RFID? Which ones? Do they have to follow specific security requirements? Which ones?

4. Applications (Mobile)

4.1. Data Protection Issues:

Information society is increasingly relying on the use of "apps" (application), most of them mobile. These apps are commonly designed to gather personal data, and in practice often process medical data.
Technologies such as multi-touch touchscreen, accelerometers or gyroscopes, ambient light sensors, GPS and cameras, and devices featuring fingerprint and biometric sensors also involve the collection of medical data.

A mobile phone application can monitor accurately physiological data, such as heartbeats, sleep patterns, fitness information.

4.2. Questions: Is your legal framework providing for a regulation of Apps and Mobile Apps? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Apps:	Is it allowed to use apps and mobile apps to deploy medical services and collect medical data? If yes, which type of individual/organisation can develop and employ these apps? Are there specific security requirements for these types of apps?
Institutions:	Do hospitals/clinics/labs employ apps to gather medical data? Is there a need for a medical treatment to permit the use of an app to process the medical data? Are there specific security requirements for the institutions collecting these data from the apps? Are medico-administrative data used by hospitals/clinics for management purposes?

Tracking technologies:	Do hospitals/clinics/labs employ non-medical apps and devices to track and collect data from their patients? What type of data is collected? For what purpose? Is the data identifiable? Is the data combined with medical data?
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical apps and tracking apps? If yes, what are the standards?
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical diagnostic? How would this be applied to fitness and daily-basis data?

5. Medical Devices and Wearable Devices

5.1. Data Protection Issues:

A medical device can be defined as: 'any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application. Such a device should be intended by the manufacturer for one of a number of defined purposes, one of which is, diagnosis, prevention, monitoring, treatment or alleviation of disease' (Directive 93/42/EEC Article 1:2)

Some eHealth and mHealth devices and apps do not fall in this definition of medical devices, as can also be the case of a software working in combination with a physical device, for instance a smartphone.

5.2. Questions: Is your legal framework providing for a regulation of Medical Devices? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
eHealth and mHealth:	Does the concept of Medical device in your country encompass services and apparels in the realm of eHealth and mHealth? What are the requirements? Should, for instance, the medical device be certified before it can be used?
Apps:	Does the concept of medical devices encompass apps? If yes, is there any regulation applicable to apps that perform medical services? Is there any regulation applicable on apps that track non-medical data that can lead to health information? If yes, what type of data?

Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical and/or wearable devices? If yes, what are the standards?
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical treatment? How would this be applied to fitness and daily-basis data?

6. Internet of Things

6.1. Data Protection Issues:

Internet of things relates to common, ordinary devices that are now, and increasingly, connected to the Internet, such as cars, fridges, ovens, microwaves, etc. All of these devices can provide data that can lead to reveal information concerning one's health. A fridge can easily inform on the type of food stored and thus the diet of an individual. One of the biggest challenges of the Internet of Things is to guarantee the right to privacy and data protection in a world where every device collects, processes, analyses and transmits the data, commonly via wireless technologies.

In the realm of medical data, the issue mainly arises when crossing seemly unrelated data that can lead to health information about an individual.

6.2. Questions: Is your legal framework providing for a regulation of the Internet of Things? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Security:	What are the security standards that need to be employed by these devices when collecting personal data?
Non-medical devices:	Are non-medical devices allowed to collect medical data, such as heart frequency? Are they allowed to cross medical data with non-medical data?
Privacy by Design:	Is there any requirement to implement privacy by design in the development of connected devices? If yes, what are the standards?

7. Electronic Doctor (online Doctor) and on-line appointments

7.1. Data Protection Issues:

The Doctor listens, talks and assesses the patient online, via a website, app, canal, sometimes including video-conference. Medical data is collected and processed, what are the security requirements and standards followed? Other websites provide for on-line appointments with doctors, which can also involve the processing of medical data.

7.2. Questions: Is your legal framework providing for a regulation of online Medical Treatment and is the on-line appointment system covered by such a framework? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Medical treatment:	Is it allowed to perform medical treatment via online services? If yes, how should the medical services be provided? Does it have to follow the same requirements of a regular physically-present medical treatment?
Medical data:	How should the data collected via a medical treatment performed online be processed? Are there specific requirements? Which ones?

Other comments and technologies
Should you wish to describe any technology, feature or trend that has not been covered by the questionnaire, please feel free to use the space provided below. Where relevant, also indicate recent legislation changes, guidelines and/or case law.

CROATIA / CROATIE

QUESTIONNAIRE

The questionnaire should ideally be completed by data protection authorities, health policy authorities, professional or patient associations as well as healthcare providers: you are invited to share it as widely as possible.

Please send your replies to dataprotection@coe.int no later than 15 December 2014.

1. Mobile Health (mHealth) and Electronic Health Records (EHR)

1.1. Data Protection Issues:

This is perhaps the biggest topic sitting at the intersection of technology and data protection. Mobile health (mHealth) and Electronic Health Records (EHR) are increasingly used in healthcare systems and provisions – it is a trend that needs to be examined.

Related to the EHR, these records are more accurate, cost-effective (in terms of storage) than paper-based notes. The concept of patient controlled/accessed EHR has been implemented in varying degrees in different countries.

Furthermore, some non-medical record can still contain health information about users and it should be considered if such records ought to be treated in a similar way to EHR.

Also, should 'medical data' as defined in Recommendation N° (97) 5 on the protection of medical data cover physical tracking data, such as pedometers or fitness data and data that can lead to medical information about an individual ?

1.2. Questions: if EHR exist in your country, is your legal framework providing for a regulation of such records? If mHealth exists in your country, is your legal framework providing for a specific regulation? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	**CIHI (Croatian Institute for Health Insurance):** The implementation of the Central Electronic health record (CEHR) called eRecord or Electronic health record (EHR) is currently in progress, and is working in a way to make use of data which are already exchanging through the system called CEZIH[1] from the following mechanisms: ePrescription, eReferral - PHC laboratory, eReferral (in CEHR or hospital when it is implemented), report after each medical exemination (for four activities), report on sick leave. Legislation: • Health Care Act, OG 150/08 - 22/14 • Law on Medical Practice, OG 121/03 and 117/08 • Law on Protection of Patients' Rights, OG 169/04 and 37/08 • Law on Personal Data Protection, OG 103/03, 118/06, 41/08, 130/11 and 106 / 12- revised text • Data Secrecy Act, OG 79/07 and 86/12

[1] Central Information System of Health of the Republic of Croatia

	• Law on Right to Access Information, OG 25/13 Basing on the Law on confidentiality of information, the Law on Protection of Personal Data and a Law on the Right to Access Information the Governing Council of the Croatian Institute for Health Insurance (hereafter: Institute) has brought an internal act on 24 May 2012 Rules of data confidentiality and Right to Access Information of the Croatian Institute for Health Insurance (hereafter: Rules of data confidentiality). Ways of keeping, storaging, collecting and disposing the medical records of patients from the mandatory health insurance in the Central Information Croatian health care (CEZIH) and method of keeping personal health records in electronic form are prescribed by the Regulations. • Rules on keeping, storaging, collecting and disposing of medical records of patients in the Central Information System of Health of the Republic of Croatia, OG 82/10 • Rules on the use and protection of data from medical records of patients in the Central Information System of Health of the Republic of Croatian, OG 14/10 • Rules on Keeping the personal health records in electronic form, OG 82/10 The sanctions in cases of violation of the confidentiality of data for the employees of the Institute are regulated by Article 21 of the Rules of data confidentiality, which establishes that the actions that are contrary to the provisions of the Rules on storage and release of classified information and non-compliance with established measures to protect data, the worker makes a serious breach of duty.
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
EHR and Medical data:	**CIHI:** What can be considered medical data in your country? Is it solely the data relating to a person's health (state, diagnosis, prognosis, medical treatment, etc.)? Is non-medical data that leads to medical information treated the same way as medical data (for instance in terms of confidentiality requirements)? Is the EHR solely constituted of data collected in a medical context or can the individual also himself or herself add information regarding his or her health?
	In terms of legal or secondary legal regulation there is no precisely definition on what is considered medical data. In practice of the Institute medical data imply those data which are related to the state of health of the insured person, and they are quite broadly defined. For example, medical information can be medical history, a discharge letter, laboratory findings, diagnostic examinations and other data relating to the state of health of the insured person.

	Purpose of EHR applications is to collect and in a consistent and ergonomic way show medical information of variety of authorized users in one place. Data which are intended for storing in central EHR, receive medical applications through already implemented mechanisms (data on prescribed remedy - ePrescription, the results of laboratory tests - eReferral in primary health care (PHC), opinion of specialists – eReferral SKZZ[2] ...) CEZIH (Central Information System of Health of the Republic of Croatia) • The system works by using the virtual private network (VPN) in the current version which connects all medical offices of primary health care, Croatian Health Insurance Institute (CIHI) and the Croatian Public Health Institute (CPHI) • Doctors and medical nurses have access through applications installed in their offices, and also the CIHI and CPHI through their own applications • On central part of CEZIH from PHC offices, a corresponding individual can connect through the installed software that has successfully passed the appropriate checking of the readiness at CIHI. Since the contracting health subjects are independently purchasing the hardware and software computer equipment, the responsibility for computer security at using a functionality of CEZIH, which also includes dealing with sensitive data, it is on the side of the contracting health subjects, or his/hers employees – which represents authorized users of CEZIH • The training for authorized users of CEZIH for work with the software are performed by software houses that have applied for a license for it. Besides software solutions for medical offices/pharmacies /laboratories, it is necessary to have software support for work with the smart card and the VPN client to ensure a secure connection to the central part of CEZIH, which can be retrieved on the website of CEZIH.
Sharing of data and Access:	Who is granted access to the EHR and how is the sharing of information (with other health care providers?) regulated? Where information is shared with pharmacists, is there a strict purpose limitation in place? How has the definition of the responsibility over the medical data been regulated?
	CIHI: Selected doctor of general / family medicine, doctor of dental medicine, specialist in dental medicine, pediatric specialist, specialist in gynecology and specialist in school medicine are required to keep personal medical records of the insured person and they are also obligated to keep documents held in electronic media from any changes, premature destruction or unauthorized use. Data from the personal health records of the insured person shall be delivered in electronic form to the central part of the integrated information system of CEZIH where they are kept.

[2] Specialist - consultative health care

	CEZIH system works in a way so that only doctor, who is limited with the Contract, can at the same time see the medical and personal information of the patient. Communication between doctors and other institutions is being protected (encrypted), and medical and administrative data are completely separated from other users on the system, which means that eg. CPHI, when collecting data on health trends, can only see medical cards, but without names and surnames of patients. The central system can be accessed only by health professional offices of PHC which CIHI reported as a member of the team (team holder, replacement, nurse). Pharmacies are obliged to apply for an authorization for pharmacists, and laboratory the requirement to obtain authorization for medical biochemists and laboratory technicians, which can be downloaded from the website of CIHI. In offices of PHC it is necessary to have a computer for doctors and computer for nurse, or computer for pharmacist and computer for lab technicians. It is highly recommended before procuring the equipment of contractual health care institutions, to first consult with the manufacturer of the software whose software solution they want to use and which received a license from CIHI after the procedure for assessing the readiness of software solutions for working with CEZIH. There are persons who are authorized and who have the right to access the information from CEZIH, and are in exclusive jurisdiction of the CIHI, CNIPH, HZZOZZR and MHSW whose workers can only use the certain information for the purpose of creating a report in accordance with current regulations, or for the purpose of creating statistic reports. Authorized persons are obliged to maintain the secrecy, or confidentiality from medical documentation of the patient in CEZIH for the duration of his/hers authorization as well as after stopping the authority under which they have a right to access that data.
Data quality:	Are the principles of legitimacy, fairness and minimisation applied to medical data? How are records kept accurate? How long is the data kept for, is the specific storage period defined for the EHR?
	CIHI: The quality and accuracy of medical data which the application of EHR shows, is exactly the same as the quality and accuracy of information that different client applications are exchanging through the system of CEZIH. If the doctors write in PHC a short reason for visiting doctor such as "hard headache", "strong hit in the head", "chronic weakness", then the review of visits would be more understandable and innovative. If a doctor of PHC completely leaves out this kind of information then the medical review will be less quality. It is same is for information about status of medical history or the opinion of a doctor where you should avoid using abbreviations and also reducing the amount of information you write down. The doctor is obliged to keep accurate, detailed and dated medical records in

	accordance with the regulations of the records in the health field, which at any time can provide sufficient information about the health condition of the patient and his/hers treatment. Your doctor or other person who is in charge of the health institution, company or other legal entities who are performing health activity are obliged to keep data about ambulance treatment of patients ten years after finishing treatment, and after that time they are obliged to act in accordance with the Regulations on keeping documentation.
Data integrity:	Are any specific methods used to ensure the integrity of the data? How are patients identified in the EHR? In the context of research, are anonymisation methods used and what safeguards exist for re-identification?
	CIHI: The point of this whole mechanism is to present the information that are exchanging through clinical subsystems (such as ePrescription, eReferral etc.), and not data from reports about these processes. This means that in the application eRecord will display only information about the prescribed medical drug that is contained in an electronic recipe, not the information written in the message after each medical review. Also there will be shown the information on issued drug which is contained in a message on realization of prescriptions (part of ePrescription mechanism), and not those from account or some other source. Therefore it shows the information on the basis on which the service has been provided to the patient or is caused as a direct result of using services. For the purpose of the research and production of different reports there are used different methods of anonymization of data, such as masking information, which is practically not possible to reidentificate.
Data security:	Where are the records stored? Is there a centralised database of EHR? What security technology is being used?
	CIHI: The data from the transactional mechanisms such as eRecipes and eReferrals, will shift into production base of eRecord independently of patient's consent on data access. In other words, this means that the mechanism of transferring data in eRecord system is carried out independently, whether the patient has given authorization to access the data or not. In that way if the patient after some time, during which no one has access to data, decides to give permission to access, there will be visible all data including those which have been collected in the meantime. Depending on which one out of four levels of authorization the patient chooses, these data are given full or limited access or the access is completely banned. The application has the administrative part with two functions: managing the patient's consent to access the data, and also printing details about accessing EHR. Access to the administrative part of the application has a doctor who the patient chooses.

	Every person who works in a field of health care in Croatia has a smart card with his/hers identification data and the security certificate. The register of medical professionals leads CPHI (Croatian Public Health Institute). Smart card – CEZIH Card and the entire PKI infrastructure has been supported by CIHI. CIHI smart card - CEZIH Card is a multifunctional smart card for personal identification, it contains a qualified digital signature; also has a magnetic stripe on the back and additional protection certificate with PIN code (which is changeable).
Rights of the person/patient concerned:	How can the right of access be exercised? How can the data be corrected? Can the person enter information in his or her own EHR? What are the legal remedies available?
	CIHI: The levels of authorisation are: • The patient does not allow access to his/hers EEC - at this level of authorization, users can find a patient, see the basic identification data but it`s shown to them that the patient didn`t give permission for access to his data, • The patient gives limited access to the data and only to selected doctors in primary health care (general / family doctor, pediatrician, dentist). Other users can only see the basics of identification data and also information that the patient didn`t give permission to access, • The patient gives full access to the data with his previously approval - only doctors of PHC (general / family doctors, pediatrician, dentist) can see all data, while the other users, after the election of a patient can see the basic identification data and also information that is necessary to ask for written consent from the patient for permission to access data. There should offer access to 1, 15 and 30 days and the ability to print statement of agreement as a document, • The patient gives his full permission to access medical card – access to data have all authorized users with the appropriate role, without further permission for access. However, an authorized user must be enabled the "special access" regardless of whether the patient has given consent to access or not. It must be clearly indicated that this approach is used only in emergency situations ("break the glass" principle when eg. when something life-threatening is happening to the patient and the doctor is unable to get his written permission, and decides that his data are absolutely necessary). The doctor is obliged to keep accurate, detailed and dated medical record in accordance with the regulations of the records concerning health, which in every moment can provide relevant information on the health condition of the patient and his/hers treatment. The doctor is obliged to present the same documentation on request of the Ministry of Health, government bodies in accordance with special regulations, the Croatian Medical Chamber or legal authority.

	Doctor is obliged to allow patient the access to all medical records relating to the diagnosis and treatment of his/hers disease, if and whenever he/she requires it. When an authorized person, in accordance with a special law takes medical documentation, he/she is obliged to give an official signed certificate of takeover with a full list of taken documents to the doctor, responsible person of the health institution/company or to any legal person performing health activities. **PDPA (Personal Data Protection Agency):** Regarding the provision of Art. 18 of the Croatian Personal Data Protection Act (OG 106/12 – consolidated text; hereinafter: PDPA), personal data in personal data filing systems shall be adequately protected from accidental or deliberate abuse, destruction, loss, unauthorized alteration or access. Furthermore, the personal data filing system controller and recipient shall undertake appropriate technical, staffing and organisational measures aimed at protecting personal data, necessary for the protection of personal data from accidental loss or destruction and from unauthorized access, unauthorized alterations, unauthorized dissemination and all other forms of abuse, and to determine the obligation of all persons entrusted with the processing of personal data to sign a confidentiality statement. It is also important to remark that the techincal data protection measeures are more specified by the Regulation on the manner of storing and special measures of technical protection of the special categories of personal data (OG 139/04) Also, according to Art. 19 of the PDPA, the personal data filing system controller shall (among other obligations), at the latest within 30 days from receiving a request about it, to every data subject or his/her legal representatives or authorised persons, allow access to the personal data filing system records and to personal data in the personal data filing system relating to the data subject, and allow the copying of such files.
Consent:	Is the system based on an opt-in approach? Is the principle of granular consent applied (with the possibility of preventing access to certain data?)? If yes, in which situations?
	CIHI: The patient will be offered a choice of giving a written consent to her/his most important data from the medical card to be available to other health specialists (eg. Emergency medicine, dentistry, etc.), and also he/she can deny, in a written form, the right to access information to other health specialists in the Republic of Croatia.
Withdrawal:	Are patients able to withdraw the consent given to EHR schemes? If yes, what is the relevant procedure to withdraw such consent? What are the consequences?
	CIHI: The patient will be given a choice to withdraw their consent at any time (eg. on the return from summer vacation or a trip), and allow only their general/family doctors to have access to data from their card.

	PDPA: According to Art. 2, para 1, point 8, of the PDPA data subject's consent is any freely given and clear consent by which the data subject indicates his/her approval for his/her personal data to be processed for a specific purpose. Also, the Art. 7, para. 1 of the same Act stipulates that the consent is one of the legal bases for personal data collection and subsequently processing. In relation with that, Art. 7, para. 2, stipulates that the data subject has the right to revoke his/her consent at any time, and request the termination of further processing of his/her data, unless this data is processed for statistical purposes when personal data can no longer lead to the identification of the person it relates to.
Outsourcing processing of data:	Is outsourcing common? Under what circumstances? Where is the data outsourced to? What sort of safeguards are in place?
	CIHI: Outsourcing in the processing of data does not exist.

2. Cloud Computing, Data Mining and Profiling from both Medical Records (including EHR) and Data not specifically related to medical records.

2.1. Data Protection Issues:

Cloud computing has brought a new dimension to the way data is stored, accessed and processed. Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS), Network as a service (NaaS) are all used by services and organisations that deal with both medical data and non-medical data.

With the development of more advanced and efficient data-mining and data-querying Medical techniques (e.g NoSQL, MapReduce, Hadoop) in conjunction with increased processing power and data storage, mining data has never been more informative, easier, and cost-effective.

Healthcare is a natural sector in which to apply new technologies and methodologies, with particular impacts in epidemiology, public health, health services research, etc.

Data that can lead to the identification of a particular individual and his/her health situation is not limited to medical data *per se,* present on Electronic Health Records, but also to unsuspicious type of information.

There is a growing concern that these schemes may be implemented in manner which does not always respect the patients' confidentiality and basic rights, and in a broader context, the use of this of information may prejudice the individuals concerned.

The ability to track and monitor patients and resources enables a more efficient provision of care but may have an impact on the right to privacy of the individual concerned.

2.2. Questions: Is your legal framework providing for a regulation of Cloud Computing, Data Mining and Profiling? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	**PDPA:** This issue is not specifically regulated by the Croatian legislation. Therefore the general data protection provisions apply to cloud computing. The most relevant PDPA provisions for this case are the following: - The personal data filing system controller shall process personal data only under conditions stipulated by the PDPA and special acts. (Art 5) - Personal data may be collected for a purpose known to the data subject, explicitly stated and in accordance with the law, and may be subsequently processed only for the purposes it has been collected for, or for a purpose in line with the purpose it has been collected for. Further processing of personal data for historical, statistical or scientific purposes shall not be considered as incompatible provided that appropriate protection measures are in place. Personal data must be relevant for the accomplishment of the established purpose and shall not be collected in quantities more extensive than necessary for achieving the purpose defined. Personal data must be accurate, complete and up-to-date. Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data was collected or for which it is further processed. Appropriate protection measures for personal data stored for longer periods of time for historical, statistical or scientific usage are established by special acts. The personal data filing system controller is responsible for implementing provisions of this Article. (Art 6) - Special categories of personal data may only be processed - upon consent of the data subject, or if the data processing is necessary to exercise the rights and obligations of the personal data filing system controller based on special regulations, or if the processing is necessary for the protection of life or physical integrity of another person, when the data subject is unable to provide his/her consent for physical or legal reasons, or if the processing is carried out within the scope of legal activity of an institution, association or any other non-profit entity with political, religious or other aim, provided that such processing relates solely to the members of this entity, and that the data obtained is not disclosed to a third party without prior consent of the data subject, or if data processing is necessary to establish, obtain or protect claims prescribed by law, or when the data subject personally published this data, or if data processing is necessary for the purpose of preventive medicine, medical diagnosis, health care or management of health institutions, on the condition that the data is processed by a health official based on rules and regulations adopted by competent authorities. (Art 8) Also, with regard to this issue, applies the provision on data transfer (Art 13): - Personal data filing systems or personal data contained in personal data filing systems may be transferred abroad from the Republic of Croatia for further processing only if the state or the international organization the personal data is being transferred to have adequately regulated the legal protection of personal data and have ensured an adequate level of protection. Prior to transferring

	personal data abroad from the Republic of Croatia, the personal data filing system controller shall, in case of reasonable doubt that an adequate personal data protection system exists, or that the adequate level of protection is ensured, obtain an opinion regarding this issue from the Personal Data Protection Agency. Exceptionally, personal data forming part of personal data filing systems may be taken out of the Republic of Croatia to states or to international organizations which do not provide for an adequate level of protection only in the following cases: if the data subject consents to the transfer of his/her personal data only for the purpose for which the he/she provided consent, or if the transfer is essential for protecting the life or the physical integrity of the data subject, or if the personal data filing system controller provides sufficient guarantees regarding the protection of privacy and the fundamental rights and freedoms of individuals, which might arise from contractual provisions, for which the Personal Data Protection Agency establishes that they comply with regulations in force governing personal data protection, or if the transfer of data is necessary for the execution of contract between the personal data filing system controller and the data subject, or for the implementation of pre-contractual measures undertaken upon data subject's request, or if the data transfer is necessary for the conclusion or execution of a contract between the personal data filing system controller and a third person, and which is in the interest of the data subject, or if the data transfer is necessary or determined by law for protecting public interest or to establish, obtain or protect the claims prescribed by law, or if data is transferred from records the purpose of which, based on the law or another regulation, is to provide public information, and which is available to the public or to any person who can prove a legal interest in it, data may be transferred to the point to which requirements determined for review in a particular case have been prescribed by law. The PDPA provides the following sanctions (Art. 36) that could be applied in relation to cloud computing: A fine of HRK 20,000.00 to 40,000.00 shall be charged for the following violations (the person responsible within the legal person, or in the state administration body and in the local and regional self-government unit shall also be fined for the violations from paragraph 1 of this Article in the amount of HRK 5,000.00 to 10,000.00): - if a processor exceeds his/her authority or collects personal data for a purpose other than that agreed, or discloses them for usage to other recipients or does not ensure the implementation of appropriate personal data protection measures, - if a personal data filing system controller or the recipient fail to ensure adequate personal data protection, - if a personal data filing system controller does not, upon request of the data subject, supplement, amend or delete incomplete, incorrect or obsolete data, - if the personal data filing system controller, the recipient or processing official prevent the Agency from conducting activities

	- if the personal data filing system controller or processing official fail to respect an order or a prohibition issued by the Agency
Case-law:	
Other:	
Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Cloud computing:	How is cloud computing regulated in your country? Which security safeguards and standards are mandatory? Are there specific requirements in order to store medical data in the cloud? How is data shared and is the sharing regulated?
	PDPA: This issue is not specifically regulated by the Croatian legislation. Therefore the general data protection provisions apply to cloud computing. In this regard applies especially the Regulation on the manner of storing and special measures of technical protection of the special categories of personal data (OG 139/04), as well as the following Articles of the PDPA: Art. 10: - Based on a contract, the personal data filing system controller may entrust individual tasks regarding the processing of personal data within his/her authority to other natural or legal persons (hereinafter: processor). Tasks regarding personal data processing may be entrusted solely to a processor registered for conducting these activities, who provides sufficient guarantees that appropriate personal data protection measures will be implemented or classified data when he/she fulfils the requirements determined by special regulations governing the field of information security. - The contract shall regulate mutual rights and obligations of the personal data filing system controller and the processor, where the processor is in particular under the obligation to: act only pursuant to an order issued by the personal data filing system controller, not provide personal data to other recipients for usage, nor process it for any other purpose than that defined by the contract, ensure that the appropriate technical, organizational and staffing measures are in place for personal data protection, in accordance with provisions stipulated by the PDA. The contract from paragraph 1of this Article shall be drawn up in writing. Art. 18: Personal data in personal data filing systems shall be adequately protected from accidental or deliberate abuse, destruction, loss, unauthorized alteration or access. The personal data filing system controller and recipient shall undertake appropriate technical, staffing and organizational measures aimed at protecting personal data, necessary for the protection of personal data from accidental loss or destruction and from unauthorized access, unauthorized alterations, unauthorized

	dissemination and all other forms of abuse, and to determine the obligation of all persons entrusted with the processing of personal data to sign a confidentiality statement. Protection measures must be proportionate to the nature of activities of the personal data filing system controller or the recipient, and to the contents of the personal data filing systems. Also, the following provisions of the Electronic Communications Act (Art. 99 – OG 73/08, 90/11, 133/12, 80/13, 71/14) also apply: Operators of public communications services must take appropriate technical and organisational measures to safeguard security of their services, and, together with the operators of public communications networks take the necessary measures with respect to security of the electronic communications network. Having regard to the available technical and technological solutions and the costs of their implementation, these measures shall ensure a level of security appropriate to the network security risk presented. In case of a particular risk of a breach of the security of the network, the operator of publicly available electronic communications services must inform the users of its services about such risk. Where the risk lies outside the scope of the measures to be taken by the operator of publicly available electronic communications services, users must be informed about any possible measures for the elimination of the risk and/or consequences thereof, including an indication of the likely costs involved.
Government:	Do governmental programmes exist to allow for increased data-mining of medical records? If yes, what are the purposes of this data mining? Are private entities allowed to access the data? Under what circumstances? What sort of techniques and technologies are being used? To what end? Are data subjects informed of this type of data-mining?
Private sector:	Are private entities allowed to mine medical data which they process? Under what circumstances? Can the government have access to this data?
Profiling:	Are the government and the private sector allowed to employ profiling methods on medical data? If yes, under what circumstances? Is it allowed to cross and correlate non-medical data with medical data?

3. RFID and wireless communication technologies

3.1. Data Protection Issues:

It is common for medical devices, such as patients' tags, to possess RFID technologies in order to facilitate the transmission of the patients' data.

It can also be related to the data-mining operations previously mentioned as it is another category of

information that can be used to discern meaningful patterns. Transmission of data through radio-frequency is not limited to medical devices. Almost any smartphone uses some technology enabling to collect, and share, the user's data. For instance, via WI-FI it is possible to identify users' locations and therefore infer some of their behaviour, which in some cases can relate to health information.

3.2. Questions: Is your legal framework providing for a regulation of RFID technologies and the transfer of personal data through wireless technologies? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	**PDPA:** This issue is not specifically regulated by the Croatian legislation. Therefore the general data protection provisions apply to RFID. The most relevant PDPA provisions for this case are the same as listed in question 2.2.
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
RFID:	How is RFID used in hospital/clinics for (a) resource management, (b) patient care? What types of database systems (and security) are implemented in conjunction with RFID use? How are issues of access, sharing, consent etc. managed considering that RFID may be used without the patient`s knowledge.
Wireless tracking technologies:	Are hospitals/clinics employing other wireless tracking technologies besides RFID? Which ones? Do they have to follow specific security requirements? Which ones?

4. Applications (Mobile)

4.1. Data Protection Issues:
Information society is increasingly relying on the use of "apps" (application), most of them mobile. These apps are commonly designed to gather personal data, and in practice often process medical data. Technologies such as multi-touch touchscreen, accelerometers or gyroscopes, ambient light sensors, GPS and cameras, and devices featuring fingerprint and biometric sensors also involve the collection of medical data. A mobile phone application can monitor accurately physiological data, such as heartbeats, sleep patterns, fitness information.

4.2. Questions: Is your legal framework providing for a regulation of Apps and Mobile Apps? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	**PDPA:** This issue is not specifically regulated by the Croatian legislation. Therefore the general data protection provisions apply to applications and mobile applications. The most relevant PDPA provisions for this case are the same as listed in question 2.2.
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Apps:	Is it allowed to use apps and mobile apps to deploy medical services and collect medical data? If yes, which type of individual/organisation can develop and employ these apps? Are there specific security requirements for these types of apps?
Institutions:	Do hospitals/clinics/labs employ apps to gather medical data? Is there a need for a medical treatment to permit the use of an app to process the medical data? Are there specific security requirements for the institutions collecting these data from the apps? Are medico-administrative data used by hospitals/clinics for management purposes?
Tracking technologies:	Do hospitals/clinics/labs employ non-medical apps and devices to track and collect data from their patients? What type of data is collected? For what purpose? Is the data identifiable? Is the data combined with medical data?
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical apps and tracking apps? If yes, what are the standards?
	PDPA: Information on requirements to implement privacy by design is not available. It is remarkable that the implemented measures shall comply (among other) with the following PDPA provisions: Art. 6: Personal data may be collected for a purpose known to the data subject, explicitly stated and in accordance with the law, and may be subsequently processed only for the purposes it has been collected for, or for a purpose in line with the purpose

	it has been collected for. Further processing of personal data for historical, statistical or scientific purposes shall not be considered as incompatible provided that appropriate protection measures are in place. Personal data must be relevant for the accomplishment of the established purpose and shall not be collected in quantities more extensive than necessary for achieving the purpose defined. Personal data must be accurate, complete and up-to-date. Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data was collected or for which it is further processed. Appropriate protection measures for personal data stored for longer periods of time for historical, statistical or scientific usage are established by special acts. The personal data filing system controller is responsible for implementing provisions of this Article. Art. 18: Personal data in personal data filing systems shall be adequately protected from accidental or deliberate abuse, destruction, loss, unauthorized alteration or access. The personal data filing system controller and recipient shall undertake appropriate technical, staffing and organisational measures aimed at protecting personal data, necessary for the protection of personal data from accidental loss or destruction and from unauthorized access, unauthorized alterations, unauthorized dissemination and all other forms of abuse, and to determine the obligation of all persons entrusted with the processing of personal data to sign a confidentiality statement. Protection measures must be proportionate to the nature of activities of the personal data filing system controller or the recipient, and to the contents of the personal data filing systems. Also, there should be taken into consideration that the special categories of personal data can be processed only exceptionally as stated in Art. 8 of the PDPA (see question 2.2). Also, the following provisions of the Electronic Communications Act (Art. 99 – OG 73/08, 90/11, 133/12, 80/13, 71/14) also apply: Operators of public communications services must take appropriate technical and organisational measures to safeguard security of their services, and, together with the operators of public communications networks take the necessary measures with respect to security of the electronic communications network. Having regard to the available technical and technological solutions and the costs of their implementation, these measures shall ensure a level of security appropriate to the network security risk presented. In case of a particular risk of a breach of the security of the network, the operator of publicly available electronic communications services must inform the users of its services about such risk. Where the risk lies outside the scope of the measures to be taken by the operator of publicly available electronic communications services, users must be informed about any possible measures for the elimination of the risk and/or consequences thereof, including an indication of the likely costs involved.

Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical diagnostic? How would this be applied to fitness and daily-basis data?
	PDPA: Yes, and therefore for data processing is necessary the informed consent of the data subject. It is not necessary to be in reference to a medical treatment, but anyway there should be a legal basis for collection and further processing. As mentioned before, an informed consent should cover it.

5. Medical Devices and Wearable Devices

5.1. Data Protection Issues:

A medical device can be defined as: 'any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application. Such a device should be intended by the manufacturer for one of a number of defined purposes, one of which is, diagnosis, prevention, monitoring, treatment or alleviation of disease' (Directive 93/42/EEC Article 1:2)

Some eHealth and mHealth devices and apps do not fall in this definition of medical devices, as can also be the case of a software working in combination with a physical device, for instance a smartphone.

5.2. Questions: Is your legal framework providing for a regulation of Medical Devices? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	**PDPA:** This issue is not specifically regulated by the Croatian legislation. Therefore the general data protection provisions apply to applications and mobile applications. The most relevant PDPA provisions for this case are the same as listed in question 2.2.
Case-law:	
Other:	**CIHI** (AMPMD - Agency for Medicinal Products and Medical Devices): Data on medical devices class risk I are enrolled in the Register of Medicinal Products in Agency for Medical Products and Medical Devices and also the medical devices class risk IIa, IIb and III which are on the Croatian market. Database of Medical Devices can be searched out according to one or more criteria: name of the medical product; date of medical decision; the purpose of the medical device; manufacturer of medical products; the applicant or notification; class of issued document; reg. No. of issued document; risk classes of medical product. The medical product is intended for: - diagnosing, preventing, tracking, treatment and alleviating disease

	- diagnosing, tracking, treatment, control, reduce or eliminate injury or handicap - testing, removing, replacing or moderating the anatomy and physiological functions of the organism - controling the conception

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
eHealth and mHealth:	Does the concept of Medical device in your country encompass services and apparels in the realm of eHealth and mHealth? What are the requirements? Should, for instance, the medical device be certified before it can be used?
	CIHI (CAMS - Croatian Academy of Medical Sciences): Declaration on e-health, Croatian Academy of Medical Sciences (CAMS), Zagreb, April 2011. **http://www.amzh.hr/novosti%20i%20dogadaji.html#_1.** E-Health is the common name for the development, implementation and evaluation of Information and communication technologies (ICT) in the health system for needs of health professionals (routine or professional work; continuous education and lifelong learning; evaluation on professional work and researches) and for the needs of all citizens (care for their own health; informing about the functioning of health systems; the reliability of health information on the Internet). Nowadays there are different terms about use of ICT in health and medicine (biomedical, medical and health informatics, portals about health; medical advices on Internet; information for patients; computerization of Health care; internetization of Health care; telemedicine). It is useful to create a term that includes all of above, and that`s e-Health. Certification of programming and other solutions: Before being used each product must pass the certification process - checking functionality, safety of data, systems and interoperability. For that purpose it is necessary to set the primary criteria which a product must possess, establish a body that will implement the certification process, define the period for which the certificate will be valid as well as the conditions for a potential re-certification of products. When it comes to the HIS (Health Information System), EHR (Electronic Health Record), etc., the body that implements certification must include a different professions: 1. users of/and health professionals, 2. medical Informatics and ICT professionals, 3. lawyers and 4. different professions and individuals who are potentially interested in the considered problems.

CIHI (AQAHSC - Agency for Quality and Accreditation in Health and Social Care):

Medical technology implies a medical drug, medical device or medical procedure used for the prevention, diagnosis, treatment or rehabilitation of individual.

The evaluation of health technologies (Health Technology Assessment, HTA) represents a comparison of new and existing health technologies with the technology that is used in practice or is considered the best possible ("gold standard") on the basis of clinical efficacy and safety, economic analyzes, ethical, legal, social and organizational principles.

The main purpose of health technology evaluation is giving recommendation for making a decision about the justification of the application of new technologies or replacing existing health technologies. Recommendation on the justification of using new or replacing existing health technology is impartial, professional, objective and transparent.

Procedure of evaluation of health technologies performed by the Agency for quality and accreditation in health and social welfare (Department of development, research and health technology), based on Article 36 of the Law on the quality of health care and social welfare, OG 124/11. The Agency is processing the implementation according the "Croatian guidelines for the evaluation of health technologies".

The evaluation of health technology can refer to:

- The estimate of one technology for one indication (Single Technology Assessment, STA) compared to best one existing.
- The estimate of multiple technologies for one indication or one technology for multiple indication (Multiple Technology Assessment, STA) compared to best one existing.

The final product of evaluation of health technology represents a written document - a recommendation which includes the following components (domains):

- Description of health problems and treatment,
- Description of new health technologies and technology comparisons,
- Clinical effectiveness,
- Security,
- Cost and economic evaluation,
- Ethical principles,
- The organizational principles,
- Social principles,
- Legal principles.

Apps:	Does the concept of medical devices encompass apps? If yes, is there any regulation applicable to apps that perform medical services? Is there any regulation applicable on apps that track non-medical data that can lead to health information? If yes, what type of data?
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical and/or wearable devices? If yes, what are the standards?
	PDPA: Information on requirements to implement privacy by design is not available. Please see the general requirements under question 4 – privacy by design.
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical treatment? How would this be applied to fitness and daily-basis data?
	PDPA: Yes, and therefore for data processing is necessary the informed consent of the data subject. It is not necessary to be in reference to a medical treatment, but anyway there should be a legal basis for collection and further processing. As mentioned before, an informed consent should cover it.

6. Internet of Things

6.1. Data Protection Issues:

Internet of things relates to common, ordinary devices that are now, and increasingly, connected to the Internet, such as cars, fridges, ovens, microwaves, etc. All of these devices can provide data that can lead to reveal information concerning one's health. A fridge can easily inform on the type of food stored and thus the diet of an individual. One of the biggest challenges of the Internet of Things is to guarantee the right to privacy and data protection in a world where every device collects, processes, analyses and transmits the data, commonly via wireless technologies.

In the realm of medical data, the issue mainly arises when crossing seemly unrelated data that can lead to health information about an individual.

6.2. Questions: Is your legal framework providing for a regulation of the Internet of Things? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	**PDPA:** This issue is not specifically regulated by the Croatian legislation. Therefore the general data protection provisions apply to Internet of things. The most relevant PDPA provisions for this case are the same as listed in question 2.2.
Case-law:	

Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Security:	What are the security standards that need to be employed by these devices when collecting personal data?
	According to Art. 18 of the **PDPA**: Personal data in personal data filing systems shall be adequately protected from accidental or deliberate abuse, destruction, loss, unauthorized alteration or access. The personal data filing system controller and recipient shall undertake appropriate technical, staffing and organizational measures aimed at protecting personal data, necessary for the protection of personal data from accidental loss or destruction and from unauthorized access, unauthorized alterations, unauthorized dissemination and all other forms of abuse, and to determine the obligation of all persons entrusted with the processing of personal data to sign a confidentiality statement. Protection measures must be proportionate to the nature of activities of the personal data filing system controller or the recipient, and to the contents of the personal data filing systems. Also the Regulation on the manner of storing and special measures of technical protection of the special categories of personal data (OG 139/04) is applied.
Non-medical devices:	Are non-medical devices allowed to collect medical data, such as heart frequency? Are they allowed to cross medical data with non-medical data?
	PDPA: Yes, both options possible if PDPA requirements are fulfilled.
Privacy by Design:	Is there any requirement to implement privacy by design in the development of connected devices? If yes, what are the standards?
	PDPA: Information on requirements to implement privacy by design is not available. Please see the general requirements under question 4 – privacy by design.

7. Electronic Doctor (online Doctor) and on-line appointments

7.1. Data Protection Issues:

The Doctor listens, talks and assesses the patient online, via a website, app, canal, sometimes including video-conference. Medical data is collected and processed, what are the security requirements and standards followed? Other websites provide for on-line appointments with doctors, which can also involve the processing of medical data.

7.2. Questions: Is your legal framework providing for a regulation of online Medical Treatment and is the on-line appointment system covered by such a framework? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	**PDPA:** This issue is not specifically regulated by the Croatian legislation. Therefore the general data protection provisions apply to on-line medical services. The most relevant PDPA provisions for this case are the same as listed in question 2.2.
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Medical treatment:	Is it allowed to perform medical treatment via online services? If yes, how should the medical services be provided? Does it have to follow the same requirements of a regular physically-present medical treatment?
	CIHI: (CIT - Croatian Institute for Telemedicine) Telemedicine is providing medical care from the distance. It is all about the transfer of information from the distance between the two sides: the patient and a doctor or between healthcare professionals. Using the most advanced information and communications technology, by using cameras, screens and medical diagnostic devices, enables the simultaneous connections of patients and medical specialists, no matter the distance. Medical services that can provide the medical examination, diagnosis with help of special medical equipment and therapies. Telemedical-examination is same as a regular medical examination, except in his way you will see and talk to specialist through screens and cameras. Specialist with whom you have agreed a medical examination will have the most information about you before your even arrive, but sometimes it may be necessary to bring some medicines or medical reports. During telemedicine views there is present a healthcare professional qualified to work with telemedicine equipment, because he needs to visualize your state of health through specific medical equipment that is needed specifically for your medical review.
Medical data:	How should the data collected via a medical treatment performed online be processed? Are there specific requirements? Which ones?
	CHI: CIT As same as the regular examination by a doctor of medicine, telemedicine examination is private and confidential. Only patients and their possible accompaniment can have access to data, and possible health care professionals involved in the medical examination. Technology that is used in order to convey information between users in urban, rural and hard to reach areas in a safe way. Croatian Institute for telemedicine is a public, topic and professional institution founded to promote the use of new techniques and technologies for the diagnosis and treatment at the distance in the Republic of Croatia according to the Amendments to the Act on Law on Health Care.

Other comments and technologies
Should you wish to describe any technology, feature or trend that has not been covered by the questionnaire, please feel free to use the space provided below. Where relevant, also indicate recent legislation changes, guidelines and/or case law.

ESTONIA / ESTONIE

QUESTIONNAIRE

1. Mobile Health (mHealth) and Electronic Health Records (EHR)

1.1. Data Protection Issues:

This is perhaps the biggest topic sitting at the intersection of technology and data protection. Mobile health (mHealth) and Electronic Health Records (EHR) are increasingly used in healthcare systems and provisions – it is a trend that needs to be examined.

Related to the EHR, these records are more accurate, cost-effective (in terms of storage) than paper-based notes. The concept of patient controlled/accessed EHR has been implemented in varying degrees in different countries.

Furthermore, some non-medical record can still contain health information about users and it should be considered if such records ought to be treated in a similar way to EHR.

Also, should 'medical data' as defined in Recommendation N° (97) 5 on the protection of medical data cover physical tracking data, such as pedometers or fitness data and data that can lead to medical information about an individual ?

1.2. Questions: if EHR exist in your country, is your legal framework providing for a regulation of such records? If mHealth exists in your country, is your legal framework providing for a specific regulation? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	The governing act is Health Services Organisation Act[3], specifically chapter 5[1](Health Information System). Government of the Republic established the Health Information System and its statutes with a regulation - Statute of Health Information System (governments Statute no 131 August 14th 2008)[4]. The Statute no 53 September 17th 2008 of Ministry of Social Affairs on The Composition of Data, Conditions and Order of Maintaining of the Documents Forwarded to the Health Information System. E-prescription system is regulated with Medicinal Products Act and the governments Statute no 130 August 14th 2008. State supervision over the Health Information System is conducted by the chief processor (Ministry of Social Affairs), Estonian Information System's Authority (Riigi Infosüsteemi Amet)[5], Data Protection Inspectorate and Health Board (Terviseamet). All the processing of personal data is logged in the Health Information System. No specific legislation for mHealth from the state side, therefore the general requirements for data processing derive from the Personal Data Protection Act[6].
Case-law:	Law of Obligations Act[7] § 768 (1): Providers of health care services and persons participating in the provision of health care services shall maintain the confidentiality of information regarding the identity of patients and their state of health which has become known to them in the course of providing health care

[3] https://www.riigiteataja.ee/en/eli/520102014006/consolide
[4] https://www.riigiteataja.ee/akt/110052014031 (only in Estonian)
[5] Supervisory competence derives from Public Information Act (https://www.riigiteataja.ee/en/eli/510072014004/consolide) §53[1].
[6] https://www.riigiteataja.ee/en/eli/509072014018/consolide
[7] https://www.riigiteataja.ee/en/eli/516092014001/consolide

	services or performing their official duties and they shall ensure that the information contained in documents specified in § 769 of this Act[8] does not become known to other persons unless otherwise prescribed by law or by agreement with the patient. Health care providers, who have the obligation to maintain confidentiality arising from law, have the right to process personal data required for the provision of a health service, including sensitive personal data, without the permission of the data subject. The data processing is also permitted if it is processed with the data subject's informed consent. Health care provider does not have the right to process data subject's personal data for personal goals. If a health care provider processes data subject's personal data without the data subject's consent and the processing is not carried out to provide a health service, then the data processor breaches the Health Services Organisation Act and Personal Data Protection Act. Data Protection Inspectorate supervises according to the Personal Data Protection Act. Sanctions are stipulated in the Personal Data Protection Act §§ 42 and 43. A fine up to 300 fine units (for a natural person) is 1200 euros. Illegal disclosure of patient's personal data may in some cases be a criminal offence – see Penal Code[9] §§ 157 and 157[1]. The legislator has reassessed the Penal Code[10] §§ 157 and 157[1] and after 01.01.2015[11] the necessary elements of the offence are changed to misdemeanours (except in case of § 157[1] (2) and (4)). After 01.01.15 the offence is a misdemeanor if the case is following: illegal disclosure of sensitive personal data, enabling access to such data or transfer of such data. The case is a criminal offence if the same elements of the offence are met with and it is being done for personal gain or if damage is caused to another person.
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
EHR and Medical data:	What can be considered medical data in your country? Is it solely the data relating to a person's health (state, diagnosis, prognosis, medical treatment, etc.)? Is non-medical data that leads to medical information treated the same way as medical data (for instance in terms of confidentiality requirements)? Is the EHR solely constituted of data collected in a medical context or can the individual also himself or herself add information regarding his or her health?
	Personal Data Protection Act § 4 (1): Personal data are any data concerning an identified or identifiable natural person, regardless of the form or format in which such data exist. Personal Data Protection Act § 4 (2) p 3: The following are sensitive personal data: data on the state of health or disability. Ministry of Social Affairs and Estonian eHealth Foundation[12]: Medical data is the data related to the healthcare services provided by health care professionals (state, diagnosis, prognosis, medical treatment, etc.) The conditions and procedure for maintaining records of the provision of health services is regulated by law. If non-medical data contains sensitive data – the data should be kept confidentially.

[8] A provider of health care services shall document the provision of health care services to each patient pursuant to the requirements and shall preserve the corresponding documents. The patient has the right to examine these documents and to obtain copies thereof at his or her own expense, unless otherwise provided by law.
[9] https://www.riigiteataja.ee/en/eli/521082014001/consolide
[10] https://www.riigiteataja.ee/en/eli/521082014001/consolide
[11] https://www.riigiteataja.ee/akt/112072014005 (only in Estonian)
[12] http://www.e-tervis.ee/index.php/en/

	DPA finds that the non-medical data that leads to medical information needs to be treated the same way as medical data, because this data may reveal the patient's sensitive data and therefore cause damage to person. The health care providers add the personal data to the Health Information System, but the patient can also add personal data about him/her: e.g. Health Services Organisation Act § 59^2 (1^2). Individuals are allowed to add/change information concerning only general data (contact details). The System's statute states that a person has the right to submit (and rectify) personal data to the System if the source of data in the System are the patient's statements.
Sharing of data and Access:	Who is granted access to the EHR and how is the sharing of information (with other health care providers?) regulated? Where information is shared with pharmacists, is there a strict purpose limitation in place? How has the definition of the responsibility over the medical data been regulated?
	All healthcare providers must send data to EHR. Access only to licensed medical professionals – the attending doctor concept. ID card for authentication and digital signature Granting access to data in Health Information System is stipulated in the Health Services Organisation Act § 59^3. And specific regulation is in the statute of the Health Information System. Chief processor of Digital Prescription Centre forwards to the Health Information System following data: data of the delivered medicinal product and data of the medical prescription. With pharmacist information is shared via Prescription Centre. Pharmacist do not have access to EHR. The responsibility is regulated by law (Health Services Organisation Act).
Data quality:	Are the principles of legitimacy, fairness and minimisation applied to medical data? How are records kept accurate? How long is the data kept for, is the specific storage period defined for the EHR?
	The principles of legitimacy, fairness and minimization are applied to medical data. There is a regulation in place how to store medical data. The patient has access to his/her personal data electronically and he/she can request rectification of his/her data from the person who submitted the personal data to the Health Information System. All the processing of personal data is logged in the Health Information System (state regisrty). The logs are kept permanently in the Health Information System. Storage period for data in the Health Information System is permanent (unless the law states otherwise). Medical images are kept in the System 30 years, except medical images for dental purposes are kept 15 years. For health care providers there is a specific period for specific documents. The health care providers also have the duty to retain personal data, but in their case the retention period different – in some cases up to 110 years[13]. See also Health Services Organisation Act § 4^2.
Data integrity:	Are any specific methods used to ensure the integrity of the data? How are patients identified in the EHR? In the context of research, are anonymisation methods used and what safeguards exist for re-identification?
	Standard rules for data processing: HL7 (for medical documents) and DICOM (Picture Archive). Patients are identified by personal identification code[14]. Anonymisation is used in the context of research. Coding/recoding systems are applied in order to ensure anonymisation. Processing of personal data for scientific research or official statistics needs is

[13] https://www.riigiteataja.ee/akt/125112014008 (in Estonian)
[14] https://www.riigiteataja.ee/en/eli/518062014012/consolide § 49

	regulated in the Personal Data Protection Act § 16. Also see Health Services Organisation Act § 59^3 (5^1) and § 59^4.
Data security:	Where are the records stored? Is there a centralised database of EHR? What security technology is being used?
	Records are stored in centralized database of Estonian E-Health Foundation[15] and also in the infrastructure of hospitals/clinics. Central database is using many different security principles, for example: - (transparent) database encryption; - digitally signing/stamping records; - data quality validation; - separation of duties and validation of database quering (4-eye principle) in the backend; - principle of least privilege; - accountability (authentication, authorization, audit trail, tracing); - 2-factor authentication; - penetration testing of web applications; - and so on. The health service providers are obliged to forward data to the central system, but they also need to retain data that they create (see also 1.2. Data quality). For System security see: http://www.e-tervis.ee/index.php/en/health-information-system/electronic-health-record/system-security
Rights of the person/patient concerned:	How can the right of access be exercised? How can the data be corrected? Can the person enter information in his or her own EHR? What are the legal remedies available?
	A patient has access to his or her personal data in the Health Information System. Patient accesses the Health Information System with his/her personal ID-card[16]. The patient can request rectification of his/her data from the person who submitted the personal data to the Health Information System. See also Health Services Organisation Act § 59^2 (1^2). Talking about the centralized system: frontend: person must be registered as a medical employee in a registered medical service organization. backend: based on job duties and need to know + validation of database quering. Data can be corrected by the person/institution who is allowed to and who entered the data first place. Logs are followed. Individuals are allowed to add/change information concerning only general data (contact details).
Consent:	Is the system based on an opt-in approach? Is the principle of granular consent applied (with the possibility of preventing access to certain data?)? If yes, in which situations?
	All the health care providers are obligated to send data to the central system. See also Health Services Organisation Act 59^3 (1), (3) and (4). Patient has the right to prohibit the access to the personal data either to all personal data or restricting access to a specific document. Data access policy: opt out • Patient has the right to close his/her own data collected in the central database (*opt out*).

[15] http://www.e-tervis.ee/index.php/en/
[16] More info: http://www.id.ee/?lang=en&id=30470

	• Patient can access their own data (Patient's Portal) in order to protect a patient's life or health, a health care provider may set a time limit upon forwarding data to the Information System in the course of which the patient can first examine his or her personal data only through a health care professional. Patient can monitor visits to their Health information system (All actions will leave secure trail).
Withdrawal:	Are patients able to withdraw the consent given to EHR schemes? If yes, what is the relevant procedure to withdraw such consent? What are the consequences?
	Patient can express his or her wish 1) to donate cells, tissues or organs for transplantation after his or her death; 2) to donate corps for academic work; 3) about blood transfusions; 4) to name contact person; 5) to name a person who is authorized to purchase medication on behalf of the patient. To withdraw the consent the patient has to sign in patient portal. Authentication with ID card or MobileID.
Outsourcing processing of data:	Is outsourcing common? Under what circumstances? Where is the data outsourced to? What sort of safeguards are in place?
	Healthcare providers enter data to central system according to law (Health Services Organization Act; Statute of Health Information System (governments Statute no 131 August 14th 2008)), data is also provided by national registers, databases and information systems. To fulfill their obligation the Public Information Act is applied (data exchange systems).

2. Cloud Computing, Data Mining and Profiling from both Medical Records (including EHR) and Data not specifically related to medical records.

2.1. Data Protection Issues:

Cloud computing has brought a new dimension to the way data is stored, accessed and processed. Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS), Network as a service (NaaS) are all used by services and organisations that deal with both medical data and non-medical data.

With the development of more advanced and efficient data-mining and data-querying Medical techniques (e.g NoSQL, MapReduce, Hadoop) in conjunction with increased processing power and data storage, mining data has never been more informative, easier, and cost-effective.

Healthcare is a natural sector in which to apply new technologies and methodologies, with particular impacts in epidemiology, public health, health services research, etc.

Data that can lead to the identification of a particular individual and his/her health situation is not limited to medical data *per se,* present on Electronic Health Records, but also to unsuspicious type of information.

There is a growing concern that these schemes may be implemented in manner which does not always respect the patients' confidentiality and basic rights, and in a broader context, the use of this of information may prejudice the individuals concerned.

The ability to track and monitor patients and resources enables a more efficient provision of care but may have an impact on the right to privacy of the individual concerned.

2.2. Questions: Is your legal framework providing for a regulation of Cloud Computing, Data Mining and Profiling? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	Cloud Computing is not regulated by legal framework. Data mining and Profiling is regulated by Health Services Organisation Act. Personal Data Protection Act is applicable for data mining. The processing of personal data has to comply with the principles of processing personal data[17].
Case-law:	Data Protection Inspectorate supervises according to the Personal Data Protection Act. Sanctions are stipulated in the Personal Data Protection Act §§ 42 and 43. A fine up to 300 fine units (for a natural person) is 1200 euros.
Other:	DPA finds that cloud computing may pose a threat to unlawful access to personal data and in the case of health records the danger for infringement of person's rights are greater – e.g. in case where the data is being stored abroad (even outside EU) and the Cloud's owner may have access to the data stored within the Cloud. The DPA also notes that the Article 29 Data Protection Working Party has issued opinion 05/2012[18] on Cloud Computing.

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Cloud computing:	How is cloud computing regulated in your country? Which security safeguards and standards are mandatory? Are there specific requirements in order to store medical data in the cloud? How is data shared and is the sharing regulated?
	Medical data is not stored in cloud. No specific regulation, but the Personal Data Protection Act is applicable if processing is carried out in the territory of Estonian Republic. For specific mandatory measures, see aforementioned Act's chapter 4. If data is being shared it needs to have a legitimate ground – either an informed consent or the processing is provided in the law.
Government:	Do governmental programmes exist to allow for increased data-mining of medical records? If yes, what are the purposes of this data mining? Are private entities allowed to access the data? Under what circumstances? What sort of techniques and technologies are being used? To what end? Are data subjects informed of this type of data-mining?
	There is specific rules how to use medical data for the purposes of scientific research or statistics. Data subjects are not informed of data-mining if data is used through central system. Access are allowed according to the law (Health Services Organisation Act 59^3 (5^1)).
Private sector:	Are private entities allowed to mine medical data which they process? Under what circumstances? Can the government have access to this data?
	Access are allowed according to the law (Health Services Organisation Act). General rule is that the health care providers, who have the obligation to maintain confidentiality arising from law, have the right to process personal data required for the provision of a health service, including sensitive personal data, without the permission of the data subject.

[17] See Personal Data Protection Act § 6.

[18] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf

	But if the purpose of the processing changes, the processing needs to be carried out with a legitimate ground – either consent or if the processing is prescribed by the law. The government has no direct access to this data.
Profiling:	Are the government and the private sector allowed to employ profiling methods on medical data? If yes, under what circumstances? Is it allowed to cross and correlate non-medical data with medical data?
	Access are allowed according to the law (Health Services Organisation Act). There are no specific requirements whether the health care provider is governmental or private organization. They are allowed to data mine if they offer medical treatment according to the law.

3. RFID and wireless communication technologies

3.1. Data Protection Issues:

It is common for medical devices, such as patients' tags, to possess RFID technologies in order to facilitate the transmission of the patients' data.

It can also be related to the data-mining operations previously mentioned as it is another category of information that can be used to discern meaningful patterns.

Transmission of data through radio-frequency is not limited to medical devices. Almost any smartphone uses some technology enabling to collect, and share, the user's data. For instance, via WI-FI it is possible to identify users' locations and therefore infer some of their behaviour, which in some cases can relate to health information.

3.2. Questions: Is your legal framework providing for a regulation of RFID technologies and the transfer of personal data through wireless technologies? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	There is no specific RFID regulation. The topic is covered with generic data protection law (see above) which is mandatory to governmental and private organizations. The processing of personal data has to comply with the principles of processing personal data. In addition, there is mandatory information security standard ISKE (https://www.ria.ee/iske-en) and it describes several security measurements regarding wireless technologies (WiFi, bluetooth).
Case-law:	Data Protection Inspectorate supervises according to the Personal Data Protection Act. Sanctions are stipulated in the Personal Data Protection Act §§ 42 and 43. A fine up to 300 fine units (for a natural person) is 1200 euros.
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
RFID:	How is RFID used in hospital/clinics for (a) resource management, (b) patient care? What types of database systems (and security) are implemented in conjunction with RFID use? How are issues of access, sharing, consent etc. managed considering that RFID may be used without the patients' knowledge.
	The DPA, Ministry of Social Affairs and Estonian E-Health Foundation have no info for the use of RFID in hospitals/clinics.
Wireless tracking	Are hospitals/clinics employing other wireless tracking technologies besides RFID? Which ones? Do they have to follow specific security requirements? Which ones?

technologies:	The DPA, Ministry of Social Affairs and Estonian E-Health Foundation have no info for the use of other wireless tracking technologies besides RFID in hospitals/clinics..

4. Applications (Mobile)

4.1. Data Protection Issues:

Information society is increasingly relying on the use of "apps" (application), most of them mobile. These apps are commonly designed to gather personal data, and in practice often process medical data.
Technologies such as multi-touch touchscreen, accelerometers or gyroscopes, ambient light sensors, GPS and cameras, and devices featuring fingerprint and biometric sensors also involve the collection of medical data.

A mobile phone application can monitor accurately physiological data, such as heartbeats, sleep patterns, fitness information.

4.2. Questions: Is your legal framework providing for a regulation of Apps and Mobile Apps? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	Ministry of Social Affairs and Estonian E-Health Foundation: Apps and Mobile Apps with medical purpose are medical devices. Regulated by Medical Devices Act[19]. Also the Personal Data Protection Act is applicable. The processing of personal data has to comply with the principles of processing personal data.
Case-law:	Data Protection Inspectorate supervises according to the Personal Data Protection Act. Sanctions are stipulated in the Personal Data Protection Act §§ 42 and 43. A fine up to 300 fine units (for a natural person) is 1200 euros.
Other:	The DPA also notes that the Article 29 Data Protection Working Party has issued opinion 02/2013[20] on apps on smart devices and opinion 13/2011[21] on geolocation services on smart mobile devices. The DPA finds that in case of mobile apps the developer has to use privacy by design and provide a clear and understandable privacy policy for the app's user prior to installing the app.

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Apps:	Is it allowed to use apps and mobile apps to deploy medical services and collect medical data? If yes, which type of individual/organisation can develop and employ these apps? Are there specific security requirements for these types of apps?
	Ministry of Social Affairs and Estonian E-Health Foundation: Apps and Mobile Apps with medical purpose are medical devices. Regulated by Medical Devices Act.

[19] https://www.riigiteataja.ee/en/eli/526082014005/consolide
[20] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf
[21] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_en.pdf

	DPA: If an enterprise uses the app, the processing has to comply with the principles of processing personal data. The processing has to have a legitimate ground - mainly an informed consent. DPA does not know any restrictions to developing these apps, but the app should not be used for dissemination of spyware, malware or viruses.
Institutions:	Do hospitals/clinics/labs employ apps to gather medical data? Is there a need for a medical treatment to permit the use of an app to process the medical data? Are there specific security requirements for the institutions collecting these data from the apps? Are medico-administrative data used by hospitals/clinics for management purposes?
	The DPA, Ministry of Social Affairs and Estonian E-Health Foundation have no info for the use of apps in hospitals/clinics/labs. If the processing is being carried out, the processing has to comply with the principles of processing personal data in Personal Data Protection Act. The said Act stipulates the general requirements for data processing that have to comply with chapter 4 of the Act. Also if the processed data is sensitive data, the (chief) processor has to register with the DPA (see chapter 5 of the Personal Data Protection Act).
Tracking technologies:	Do hospitals/clinics/labs employ non-medical apps and devices to track and collect data from their patients? What type of data is collected? For what purpose? Is the data identifiable? Is the data combined with medical data?
	The DPA, Ministry of Social Affairs and Estonian E-Health Foundation have no info for the use of apps in hospitals/clinics/labs.
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical apps and tracking apps? If yes, what are the standards?
	Regulated by Medical Devices Act. Also see 4.2. Other.
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical diagnostic? How would this be applied to fitness and daily-basis data?
	If personal data is being processed, the consent must be in conformity of the Personal Data Protection Act §12.

5. Medical Devices and Wearable Devices

5.1. Data Protection Issues:

A medical device can be defined as: 'any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application. Such a device should be intended by the manufacturer for one of a number of defined purposes, one of which is, diagnosis, prevention, monitoring, treatment or alleviation of disease' (Directive 93/42/EEC Article 1:2)

Some eHealth and mHealth devices and apps do not fall in this definition of medical devices, as can also be the case of a software working in combination with a physical device, for instance a smartphone.

5.2. Questions: Is your legal framework providing for a regulation of Medical Devices? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	Medical Devices Act[22]
Case-law:	The DPA has supervisory competence only in the case of data processing. Data Protection Inspectorate supervises according to the Personal Data Protection Act. Sanctions are stipulated in the Personal Data Protection Act §§ 42 and 43. A fine up to 300 fine units (for a natural person) is 1200 euros. The Health Board is the extra-judicial body which conducts proceedings over requirements of the Medical Devices Act. The misdemeanors are stipulated in the latter mentioned Act's[23] §§ 38 and 39.
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
eHealth and mHealth:	Does the concept of Medical device in your country encompass services and apparels in the realm of eHealth and mHealth? What are the requirements? Should, for instance, the medical device be certified before it can be used?
	Medical Devices Act § 3 (1): Medical device shall mean any instrument, apparatus, appliance, software, material or other product used on humans, whether used alone or in a combination, including the software determined by the manufacturer specifically for diagnostic or medical treatment purposes which does not achieve its principal intended action in or on the human body by pharmacological, immunological or metabolic means, intended by the manufacturer to be used for human beings for the purpose of: 1) diagnosis, prevention, monitoring, treatment or alleviation of diseases; 2) diagnosis, monitoring, treatment, alleviation of or compensation for an injury or disability; 3) investigation or modification of the anatomy or of a physiological process or replacement of a part of body; 4) assisting or prevention of conception. Specific requirements for placing on market and putting into service of medical devices is stipulates in the chapter 2 of the Medical Devices Act. All medical devices should wear CE marking of conformity.
Apps:	Does the concept of medical devices encompass apps? If yes, is there any regulation applicable to apps that perform medical services? Is there any regulation applicable on apps that track non-medical data that can lead to health information? If yes, what type of data?
	Apps and Mobile Apps with medical purpose are medical devices. Regulated by Medical Devices Act. No regulation applicable on apps that track non-medical data.
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical and/or wearable devices? If yes, what are the standards?
	DPA has no knowledge of specific standards that are required to implement privacy by design in the development of medical and/or wearable devices, but data transmission standards should be used. If data processing is being carried out, the processing has to comply with the principles of processing personal data in Personal Data Protection Act. The said Act stipulates the general requirements for data processing that have to comply with chapter 4 of the Act. Also the devices need to be in conformity with the Medical Devices Act.

[22] https://www.riigiteataja.ee/en/eli/526082014005/consolide
[23] Medical Devices Act § 38 becomes void after 01.01.2015.

Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical treatment? How would this be applied to fitness and daily-basis data?
	Based on opt-out approach. Due to data reliability is need for reference to a medical treatment. Also see Medical Devices Act § 21[2].

6. Internet of Things

6.1. Data Protection Issues:

Internet of things relates to common, ordinary devices that are now, and increasingly, connected to the Internet, such as cars, fridges, ovens, microwaves, etc. All of these devices can provide data that can lead to reveal information concerning one's health. A fridge can easily inform on the type of food stored and thus the diet of an individual. One of the biggest challenges of the Internet of Things is to guarantee the right to privacy and data protection in a world where every device collects, processes, analyses and transmits the data, commonly via wireless technologies.

In the realm of medical data, the issue mainly arises when crossing seemly unrelated data that can lead to health information about an individual.

6.2. Questions: Is your legal framework providing for a regulation of the Internet of Things? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	The processing of personal data has to comply with the principles of processing personal data. Governmental organizations: general data protection law + mandatory information security standard ISKE (Personal Data Protection Act) Private sector organizations (hospitals/clinics): general data protection law. + Medical devices law
Case-law:	Data Protection Inspectorate supervises according to the Personal Data Protection Act. Sanctions are stipulated in the Personal Data Protection Act §§ 42 and 43. A fine up to 300 fine units (for a natural person) is 1200 euros.
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Security:	What are the security standards that need to be employed by these devices when collecting personal data?
	Governmental organizations: general data protection law + mandatory information security standard ISKE (Personal Data Protection Act). Private sector organizations (hospitals/clinics): only general data protection law. + Medical device law The processing of personal data has to comply with the principles of processing personal data and with chapter 4 of the Personal Data Protection Act.
Non-medical devices:	Are non-medical devices allowed to collect medical data, such as heart frequency? Are they allowed to cross medical data with non-medical data?
	1) not regulated 2) it has to have a legitimate ground – e.g. with the person's informed consent.
Privacy by Design:	Is there any requirement to implement privacy by design in the development of connected devices? If yes, what are the standards?

	No specific standards, but processing of personal data has to comply with the principles of processing personal data and with chapter 4 of the Personal Data Protection Act.

7. Electronic Doctor (online Doctor) and on-line appointments

7.1. Data Protection Issues:

The Doctor listens, talks and assesses the patient online, via a website, app, canal, sometimes including video-conference. Medical data is collected and processed, what are the security requirements and standards followed? Other websites provide for on-line appointments with doctors, which can also involve the processing of medical data.

7.2. Questions: Is your legal framework providing for a regulation of online Medical Treatment and is the on-line appointment system covered by such a framework? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	No specific legislation for online medical treatment, but data processing has to comply with the principles of processing personal data and with chapter 4 of the Personal Data Protection Act. Since the processed data is sensitive data, the data controller (health care provider) has to register the data processing with the DPA – see Personal Data Protection Act chapter 5. Also Health Services Organization Act is applicable. Regarding the online appointment system: Health care providers are required to submit to the Health Information System information for maintaining a waiting list pursuant to the provisions based on clause 56 (1) 4) of Health Services Organisation Act. Some health care providers have developed online appointment systems and the government is developing a central Digital Registration[24] – it shall be part of the Health Information System.
Case-law:	Data Protection Inspectorate supervises according to the Personal Data Protection Act. Sanctions are stipulated in the Personal Data Protection Act §§ 42 and 43. A fine up to 300 fine units (for a natural person) is 1200 euros.
Other:	Based on the sensitive personal data processing registration records, the online medical treatment is relatively small – e.g. one health care provider has notified that Skype is used; there are also some anonymized forums.

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Medical treatment:	Is it allowed to perform medical treatment via online services? If yes, how should the medical services be provided? Does it have to follow the same requirements of a regular physically-present medical treatment?
	The law does not prohibit performing medical treatment via online services (no regulation about telemedicine), but in serious cases, the health care providers suggest to visit the health care provider in person. The healthcare providers must follow regular requirements e.g. Health Services Organization Act.
Medical data:	How should the data collected via a medical treatment performed online be processed? Are there specific requirements? Which ones?
	The healthcare providers must follow regular requirements e.g. Health Services Organization Act. Also, see 7.2. Legislation.

[24] More info: http://www.e-tervis.ee/index.php/en/health-information-system/services

Other comments and technologies
Should you wish to describe any technology, feature or trend that has not been covered by the questionnaire, please feel free to use the space provided below. Where relevant, also indicate recent legislation changes, guidelines and/or case law.

FRANCE

French Health authorities have been informed of this consultation but, despite some kind reminders, I have not been able to obtain some formal answers yet.

Jean-Alexandre SILVY
--
Commissaire du Gouvernement auprès de la CNIL
Secrétariat général du Gouvernement

LATVIA / LETTONIE

Legislation:	**Exists EHR regulated by Government 11.03.2014. rules No. 134.**
Case-law:	**No cases about EHR.**
Other:	

Specific questions(for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
EHR and Medical data:	What can be considered medical data in your country? Is it solely the data relating to a person's health (state, diagnosis, prognosis, medical treatment, etc.)? Is non-medical data that leads to medical information treated the same way as medical data (for instance in terms of confidentiality requirements)? Is the EHR solely constituted of data collected in a medical context or can the individual also himself or herself add information regarding his or her health?
	All data which are collected by health care services provider and identifies any information about a person's health are considered as medical data.EHR solely constituted of data collected in a medical context or information given by competent authority.
Sharing of data and Access:	Who is granted access to the EHR and how is the sharing of information (with other health care providers?) regulated? Where information is shared with pharmacists, is there a strict purpose limitation in place? How has the definition of the responsibility over the medical data been regulated?
	Health care providers and competent authorities have full access to EHR. Pharmacists have only access to e-prescription data and patients have access to theirs and authorized person data. There is a strict purpose limitation in place.
Data quality:	Are the principles of legitimacy, fairness and minimisation applied to medical data?How are records kept accurate? How long is the data kept for, is the specific storage period defined for the EHR?
	Sensitive personal data processing is prohibited, except in cases where the personal data processing is necessary to protect the data subject or another person's life and health, and the data subject is physically or legally incapable of giving his consent. (Personal Data Protection Law, 11.paragraph, 3. Point) **Health information system manager ensures that edited and deleted information is saved in health information systems archive. No specific storage period defined (It is the same as for documentation in paper).**
Data integrity:	Are any specific methods used to ensure the integrity of the data? How are patients identified in the EHR? In the context of research, are anonymisation methods used and what safeguards exist for re-identification?
	In EHR patients are identified by their national identification number. In the context of research several anonymisation methods are used.
Data security:	Where are the records stored? Is there a centralised database of EHR? What security technology is being used?
	Medical records are stored in centralized national EHR database. Several security methods are used including accessibility by multi factor authentication and specialized user level authorization methods.

Rights of the person/patient concerned:	How can the right of access be exercised? How can the data be corrected? Can the person enter information in his or her own EHR? What are the legal remedies available?
	National regulatory authorities mentioned in Patient Right Act are empowered to process the data of the patient health information system to the extent necessary to achieve the patient's rights statutory purpose of the processing of patient data. Health care data can be corrected by removal of previous data and adding new one. **The person cannot enter any information in his own EHR.** **Personal Data Protection Law states that data subject has the right to request that his or her personal data be supplemented or corrected, as well as that their processing be discontinued or that the data be destroyed if the personal data are incomplete, outdated, false, unlawfully processed or are no longer necessary for the purposes for which they were collected. If the data subject is able to substantiate that the personal data are incomplete, outdated, false, unlawfully processed or no longer necessary for the purposes for which they were collected, the administrator has an obligation to rectify this inaccuracy or violation without delay and notify third persons who have previously received the processed data of such. A data subject has the right to receive a justified reply of an administrator in writing regarding examination of the request within a month from the day of submission of the relevant request.** **If an administrator fails to comply with the obligations, a data subject has the right to appeal to the Data State Inspectorate.** **An administrative act issued by an official of the Data State Inspectorate or actual action thereof may be contested to the director of the Data State Inspectorate. The administrative act issued by the director or actual action thereof, as well as a decision regarding the contested administrative act or actual action may be appealed to a court in accordance with the procedures laid down in the law.**
Consent:	Is the system based on an opt-in approach? Is the principle of granular consent applied (with the possibility of preventing access to certain data?)? If yes, in which situations?
	The system is based on an opt-out approach. A person can make informed decisions about the collection, use, and disclosure of their individually identifiable health information. **Patient has the right to prohibit everyone from accessing his health data.**
Withdrawal:	Are patients able to withdraw the consent given to EHR schemes? If yes, what is the relevant procedure to withdraw such consent? What are the consequences?
	The patients are not able to withdraw the consent given to EHR schemes.
Outsourcing processing of data:	Is outsourcing common? Under what circumstances? Where is the data outsourced to? What sort of safeguards are in place?
	Outsourcing is not used

2. Cloud Computing, Data Mining and Profiling from both Medical Records (including EHR) and Data not specifically related to medical records.

2.1. Data Protection Issues:

Cloud computing has brought a new dimension to the way data is stored, accessed and processed. Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS), Network as a service (NaaS) are all used by services and organisations that deal with both medical data and non-medical data.

With the development of more advanced and efficient data-mining and data-querying Medical techniques (e.g NoSQL, MapReduce, Hadoop) in conjunction with increased processing power and data storage, mining data has never been more informative, easier, and cost-effective.

Healthcare is a natural sector in which to apply new technologies and methodologies, with particular impacts in epidemiology, public health, health services research, etc.

Data that can lead to the identification of a particular individual and his/her health situation is not limited to medical data *per se,* present on Electronic Health Records, but also to unsuspicious type of information.

There is a growing concern that these schemes may be implemented in manner which does not always respect the patients' confidentiality and basic rights, and in a broader context, the use of this of information may prejudice the individuals concerned.

The ability to track and monitor patients and resources enables a more efficient provision of care but may have an impact on the right to privacy of the individual concerned.

2.2. Questions: Is your legal framework providing for a regulation of Cloud Computing, Data Mining and Profiling? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	**No legal framework for a regulation of Cloud Computing. (Personal data protection law). Patient Right Act and Personal Data Protection Law provides general principles of data protection which are used to assess proportionality. Principles stated in ECHR and ECJ case law ar applied When EU General Data Protection Regulation will come into force, it will be applicable in Latvia.**
Case-law:	
Other:	

Specific questions(for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Cloud computing:	How is cloud computing regulated in your country? Which security safeguards and standards are mandatory? Are there specific requirements in order to store medical data in the cloud? How is data shared and is the sharing regulated?
	No legal framework. Personal data protection principles stated in Data Protection Law are applied.
Government:	Do governmental programmes exist to allow for increased data-mining of medical records? If yes, what are the purposes of this data mining? Are private entities allowed to access the data? Under what circumstances? What sort of techniques and technologies are being used? To what end? Are data subjects informed of this type of data-mining?
	Not provided by any governmental programmes.

Private sector:	Are private entities allowed to mine medical data which they process? Under what circumstances? Can the government have access to this data?
	Private entities are allowed to mine medical data. Government can access data in accordance with basic principles of data protection and legal grounds for data processing.
Profiling:	Are the government and the private sector allowed to employ profiling methods on medical data? If yes, under what circumstances? Is it allowed to cross and correlate non-medical data with medical data?
	Medical data is not used for profiling. Non-medical data and medical data correlating is allowed to be used.

3. RFID and wireless communication technologies

3.1. Data Protection Issues:

It is common for medical devices, such as patients' tags, to possess RFID technologies in order to facilitate the transmission of the patients' data.

It can also be related to the data-mining operations previously mentioned as it is another category of information that can be used to discern meaningful patterns.

Transmission of data through radio-frequency is not limited to medical devices. Almost any smartphone uses some technology enabling to collect, and share, the user's data. For instance, via WI-FI it is possible to identify users' locations and therefore infer some of their behaviour, which in some cases can relate to health information.

3.2. Questions: Is your legal framework providing for a regulation of RFID technologies and the transfer of personal data through wireless technologies? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	**Not provided. Patient Right Act and Personal Data Protection Law provides general principles of data protection.**
Case-law:	**-**
Other:	**-**

Specific questions(for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
RFID:	How is RFID used in hospital/clinics for (a) resource management, (b) patient care? What types of database systems (and security) are implemented in conjunction with RFID use? How are issues of access, sharing, consent etc. managed considering that RFID may be used without the patients'knowledge.
	No information available
Wireless tracking technologies:	Are hospitals/clinics employing other wireless tracking technologies besides RFID? Which ones? Do they have to follow specific security requirements? Which ones?
	No information available

4. Applications (Mobile)

4.1. Data Protection Issues:

Information society is increasingly relying on the use of “apps” (application), most of them mobile. These apps are commonly designed to gather personal data, and in practice often process medical data.
Technologies such as multi-touch touchscreen, accelerometers or gyroscopes, ambient light sensors, GPS and cameras, and devices featuring fingerprint and biometric sensors also involve the collection of medical data.

A mobile phone application can monitor accurately physiological data, such as heartbeats, sleep patterns, fitness information.

4.2. Questions: Is your legal framework providing for a regulation of Apps and Mobile Apps? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs’ opinions and/or case law.	
Legislation:	**The legal framework doesn’t provide a regulation of Apps and Mobile Apps. Patient Right Act and Personal Data Protection Law provides general principles of data protection. Those principles are interpreted taking into account ECHR and ECJ case law.**
Case-law:	**No cases about regulation of Apps and Mobile Apps**
Other:	

Specific questions(for each section, please indicate where possible recent legislation changes, guidelines, DPAs’ opinions and/or case law).	
Apps:	Is it allowed to use apps and mobile apps to deploy medical services and collect medical data? If yes, which type of individual/organisation can develop and employ these apps? Are there specific security requirements for these types of apps?
	There is no National legislation acts for specifically using mobile apps for medical services. Data Protection principles for medical data processing are applied. For example, there has to be proper legitimate aim for processing of medical data.
Institutions:	Do hospitals/clinics/labs employ apps to gather medical data? Is there a need for a medical treatment to permit the use of an app to process the medical data? Are there specific security requirements for the institutions collecting these data from the apps? Are medico-administrative data used by hospitals/clinics for management purposes?
	No information available
Tracking technologies:	Do hospitals/clinics/labs employ non-medical apps and devices to track and collect data from their patients? What type of data is collected? For what purpose? Is the data identifiable? Is the data combined with medical data?
	No information available
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical apps and tracking apps? If yes, what are the standards?
	No requirements. Data Protection principles for medical data processing should be applied.
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical diagnostic? How would this be applied to fitness and daily-basis data?

	No legal framework provided

5. Medical Devices and Wearable Devices

5.1. Data Protection Issues:

A medical device can be defined as: 'any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application. Such a device should be intended by the manufacturer for one of a number of defined purposes, one of which is, diagnosis, prevention, monitoring, treatment or alleviation of disease' (Directive 93/42/EEC Article 1:2)

Some eHealth and mHealth devices and apps do not fall in this definition of medical devices, as can also be the case of a software working in combination with a physical device, for instance a smartphone.

5.2. Questions: Is your legal framework providing for a regulation of Medical Devices? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	**"Registration of medical devices, conformity assessment, distribution, operational and technical monitoring arrangements" regulated by Government 02.08.2005. rules No. 581. Patient Right Act and Personal Data Protection Law provides general principles of data protection.**
Case-law:	
Other:	

Specific questions(for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
eHealth and mHealth:	Does the concept of Medical device in your country encompass services and apparels in the realm of eHealth and mHealth? What are the requirements? Should, for instance, the medical device be certified before it can be used?
	No, it doesn't encompass services and apparels in the realm of eHealth and mHealth. **The medical device should be certified before they can be used.**
Apps:	Does the concept of medical devices encompass apps? If yes, is there any regulation applicable to apps that perform medical services? Is there any regulation applicable on apps that track non-medical data that can lead to health information? If yes, what type of data?
	The concept of medical devices doesn't encompass apps.
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical and/or wearable devices? If yes, what are the standards?
	Data Protection principles for medical data processing should be applied.
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical treatment? How would this be applied to fitness and daily-basis data?

	No legal framework provided

6. Internet of Things

6.1. Data Protection Issues:

Internet of things relates to common, ordinary devices that are now, and increasingly, connected to the Internet, such as cars, fridges, ovens, microwaves, etc. All of these devices can provide data that can lead to reveal information concerning one's health. A fridge can easily inform on the type of food stored and thus the diet of an individual. One of the biggest challenges of the Internet of Things is to guarantee the right to privacy and data protection in a world whereevery device collects, processes, analyses and transmits the data, commonly via wireless technologies.

In the realm of medical data, the issue mainly arises when crossing seemly unrelated data that can lead to health information about an individual.

6.2. Questions: Is your legal framework providing for a regulation of the Internet of Things? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	**No legislation for a regulation of the Internet of Things. Patient Right Act and Personal Data Protection Law provides general principles of data protection.**
Case-law:	
Other:	

Specific questions(for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Security:	What are the security standards that need to be employed by these devices when collecting personal data?
	No specific legal framework provided. Security standards are the same as to all devices collecting personal data. General data protection principles apply as well as Cabinet of Ministers ruling No.40 on mandatory technical and organizational requirements for protection of personal data.
Non-medical devices:	Are non-medical devices allowed to collect medical data, such as heart frequency? Are they allowed to cross medical data with non-medical data?
	No specific legal framework provided. The ability to collect data which are related to medical data depends on general data protection principles followed: legal basis, purpose limitation, proportionality, data retention, transparency and fair processing and security measures. The same applies to crossing medical data with non-medical data.
Privacy by Design:	Is there any requirement to implement privacy by design in the development of connected devices? If yes, what are the standards?
	No legal framework provided

7. Electronic Doctor (online Doctor) and on-line appointments

7.1. Data Protection Issues:
The Doctor listens, talks and assesses the patient online, via a website, app, canal, sometimes including video-conference. Medical data is collected and processed, what are the security requirements and standards followed? Other websites provide for on-line appointments with doctors, which can also involve the processing of medical data.

7.2. Questions: Is your legal framework providing for a regulation of online Medical Treatment and is the on-line appointment system covered by such a framework? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	**No legal framework provided for a regulation of online Medical Treatment. Patient Right Act and Personal Data Protection Law provides general principles of data protection.**
Case-law:	
Other:	

Specific questions(for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Medical treatment:	Is it allowed to perform medical treatment via online services? If yes, how should the medical services be provided? Does it have to follow the same requirements of a regular physically-present medical treatment?
	It is allowed, but not regulated in details. General data protection principles may be the same but as the environment is less safe, they are applied differently.
Medical data:	How should the data collected via a medical treatment performed online be processed? Are there specific requirements? Which ones?
	No specific legal framework provided

Other comments and technologies
Should you wish to describe any technology, feature or trend that has not been covered by the questionnaire, please feel free to use the space provided below. Where relevant, also indicate recent legislation changes, guidelines and/or case law.

LITHUANIA / LITHUANIE

QUESTIONNAIRE

The questionnaire should ideally be completed by health policy authorities, professional or patient associations as well as healthcare providers: you are invited to share it as widely as possible.

1. Mobile Health (mHealth) and Electronic Health Records (EHR)

1.1. Questions: if EHR exist in your country, is your legal framework providing for a regulation of such records? If m-Health exists in your country, is your legal framework providing for a specific regulation? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law).	
Legislation:	1.*The Ministry of Health of the Republic of Lithuania*: National e-Health System is regulated by the Law on the Health System of the Republic of Lithuania. Article 13[25] of this Law states that the Ministry of Health of the Republic of Lithuania is managing e-health system. 2. *National Transplant Bureau under the Ministry of Health of the Republic of Lithuania*: Article 7 of the Law on Donation and Transplantation of Human Tissues, Cells and Organs of the Republic of Lithuania provides that the Register of Donors and Recipients of Human Tissues, Cells and Organs (hereinafter - Register) is a public register established and maintained by the Government of the Republic of Lithuania. Paragraph 9 of Article 7 of this Law lays down that data stored in the Register are confidential and shall be disclosed according to the requirements of the Law on the Legal Protection of Personal Data and other legal acts. 3. *The State Data Protection Inspectorate of the Republic of Lithuania*: There is no National m-Health information system, but electronic health records are implemented in almost all health care institutions, by family doctors and etc. Personal data processing for the purpose of health care is regulated by Article 10 of the Law on Legal Protection of Personal Data as follows: Personal data on a person's health (its state, diagnosis, prognosis, treatment, etc.) may be processed by an authorised health care professional. A person's health shall be subject to professional secrecy under the Civil Code, laws regulating patients' rights and other legal acts.
Case-law:	-
Other:	-

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
EHR and Medical data:	What can be considered medical data in your country? Is it solely the data relating to a person's health (state, diagnosis, prognosis, medical treatment, etc.)? Is non-medical data that leads to medical information treated the same way as medical data (for instance in terms of confidentiality requirements)? Is the EHR solely constituted of data collected in a medical context or can the individual also himself

25

	or herself add information regarding his or her health?
	1.*The Ministry of Health of the Republic of Lithuania*: Inscriptions made by patients would not be treated as health data. 2. *National Transplant Bureau under the Ministry of Health of the Republic of Lithuania*: Register is a public register. Register objects are as follows: 1) persons who expressed consent (opposition) that their tissues, organs would be given for transplantation after their death ; 2) living donors; 3) deceased donors; 4) recipients; 5) tissues, cells, organs, transplant cases of disposal for the pickup. Data that leads to health data might be treated as data collected in a same way as medical data. 3. *The State Data Protection Inspectorate of the Republic of Lithuania*: Data like on a person's health (its state, diagnosis, prognosis, treatment, etc.) shall be treated as health data, but the same data that leads to health data might be treated as data collected in a same way as medical data.
Sharing of data and Access:	Who is granted access to the EHR and how is the sharing of information (with other health care providers?) regulated? Where information is shared with pharmacists, is there a strict purpose limitation in place? How has the definition of the responsibility over the medical data been regulated?
	1.*The Ministry of Health of the Republic of Lithuania*: The Law on the Health System provides that access to his/her data shall be executed by every person who requires that according to the requirements of the Law on Legal Protection of Personal Data 2. *National Transplant Bureau under the Ministry of Health of the Republic of Lithuania*: Access to Register data have entities specified in the Register Regulations those referred to in the Regulations providing and receiving data, information and documents in accordance with the procedure laid down in the Register Regulations. Entities who have right of access to the Register data also rights and duties of them settled in the Law on Management of State Information Resources of the Republic of Lithuania, Register Regulations and other legislation. *3. The State Data Protection Inspectorate of the Republic of Lithuania* The right of natural person to the direct access is laid down in the Law on Legal Protection of Personal Data. The data controller must provide the data subject whose personal data he/it collects directly from the latter with the following information, except where the data subject already has such information at his disposal: 1) the identity and permanent place of residence (natural person) or Company name and number and the address of the registered office (legal person) of the data controller and his representative; 2) the purposes of processing of the data subject's personal data;

	3) other additional information (the recipient and the purposes of disclosure of the data subject's personal data; the personal data which the data subject must provide and the consequences of his failure to provide the data, the right of the data subject to have access to his personal data and the right to request for rectification of incorrect, incomplete and inaccurate personal data) to the extent that is necessary for ensuring fair processing of personal data without infringing upon the data subject's rights. 2. The patient, upon presentation of the documents confirming his identity, shall be entitled to receive information about his state of health, diagnosis, methods of treatment or examination applied in the health care institution or alternatives known to the doctor, potential risks, complications, side-effects, prognosis of the treatment and other circumstances that may have an effect on the acceptance or rejection by the patient of the proposed treatment, as well as about the consequences of rejecting the proposed treatment. The doctor must give the patient this information in a comprehensible form, taking into account his age and state of health, explaining special medical terms.
Data quality:	Are the principles of legitimacy, fairness and minimisation applied to medical data? How are records kept accurate? How long is the data kept for, is the specific storage period defined for the EHR?
	1.*The Ministry of Health of the Republic of Lithuania*: As the e-Health information system is under implementation there are no any actual data in it. It is clear for the moment that qualified electronic signature will be used for signing of documents related with health. The data provider is responsible for the accuracy of data. The data must be stored not less than 3 years, in some cases 75 years or longer. 2. *National Transplant Bureau under the Ministry of Health of the Republic of Lithuania*: Obligations and rights of the entities who have access to the Register laid down in the Law on Management of State Information Resources of the Republic of Lithuania. All data providers must ensure that access to the data, information and documents organized in order to provide timely and proper records relating to the data. Logging off an object, information in the Register and Register data are stored in its' database 6 months, after that transferred to the archives of the database of the Register. The data in the archive of the database shall be stored 30 years. *3. The State Data Protection Inspectorate of the Republic of Lithuania* According to the requirements of Article 3 part 1 paragraph 3 of the Law on Legal Protection of Personal Data the data should be accurate and, where necessary, for purposes of personal data processing, kept up to date; inaccurate or incomplete data must be rectified, supplemented, erased or their further processing must be suspended. Article 30 of the Law on Legal Protection of Personal Data states that data controller should implement appropriate organizational and technical measures intended for the protection of personal data against accidental or unlawful destruction, alteration and disclosure as well as against any other unlawful processing. These measures must ensure a level of security appropriate in respect of the nature of the personal data to be protected and the risks represented by the processing and must be defined in a deswritten document (personal data processing regulations approved by the data controller, a contract concluded by the data controller and the data processor, etc.).

	General requirements for organizational and technical data protection measures No 1T-71 approved by the Director of the State Data Protection Inspectorate on 12.11.2008 shall be employed.
Data integrity:	Are any specific methods used to ensure the integrity of the data? How are patients identified in the EHR? In the context of research, are anonymisation methods used and what safeguards exist for re-identification?
	1.*The Ministry of Health of the Republic of Lithuania*: Data that will be submitted to the Central information system (ESPBI IS) will be tested with "Hash". The ID code, name and family name, date of birth, Electronic Health History Number (HER ID) shall be used for identification purposes. For the purpose of scientific medical research the data should be anonymized without possibility rebuild. 2. *National Transplant Bureau under the Ministry of Health of the Republic of Lithuania*: Requirements settled in the Law on Legal Protection of Personal Data of the Republic of Lithuania are as follows: 1) a person can only connect to the system, with its digitally signature or confirm his/her identity by other tolls (for example via e-Government electronic gates; 2) data on recipients may be submitted only to the person who is connected to the IT system using special passwords that are granted only under a confidentiality agreement. *3. The State Data Protection Inspectorate of the Republic of Lithuania* Processing of medical data in electronic files regulated by rules and procedures which are approved by an order of that particular data controller who is processing the data. National centralized e-Health information system is still on a stage of a design . There is the information system of National health insurance fund.
Data security:	Where are the records stored? Is there a centralised database of EHR? What security technology is being used?
	1.*The Ministry of Health of the Republic of Lithuania*: Health data will be stored in the health care institutions and in Central information system (ESPBI IS). Data stored in the ESPBI will be copied to the files of data center outside of premises where is located information system. The data to be send to the data center shall be transmitted in an encrypted channel. 2. *National Transplant Bureau under the Ministry of Health of the Republic of Lithuania*: Register is a public where compiled / entries are stored. Requirements on use of personal data are indicated in the laws: 1) a person can only connect to the system, with its digitally signature or confirm his / her identity via e-Government electronic gate; 2) data on recipients may be submitted only to the person who is connected to the IT system using special passwords that are granted only under the confidentiality agreement. *3. The State Data Protection Inspectorate of the Republic of Lithuania* Article 30 of the of the Law on Legal Protection of Personal Data states that data controller should implement appropriate organizational and technical measures intended for the protection of personal data against accidental or unlawful destruction, alteration and disclosure as well as against any other unlawful

	processing. These measures must ensure a level of security appropriate in respect of the nature of the personal data to be protected and the risks represented by the processing and must be defined in a written document (personal data processing regulations approved by the data controller, a contract concluded by the data controller and the data processor, etc.).
Rights of the person/patient concerned:	How can the right of access be exercised? How can the data be corrected? Can the person enter information in his or her own EHR? What are the legal remedies available?
	1.*The Ministry of Health of the Republic of Lithuania*: Any patient has possibility to connect to his/her Electronic Health History when he/she identifies himself/herself by electronic signature, identity card and etc. The patients' record cannot be changed, but he/she can write comments. 2. *National Transplant Bureau under the Ministry of Health of the Republic of Lithuania*: Register objects are Human tissues, cells and organs data of donors and recipients collected according to a procedure laid down in the Register Regulations. Register data providers are: 1) personal health care facilities, providing human tissues, cells, organ donation, procurement, testing, processing, storage, distribution and transplantation services; 2) tissue banks; 3) personal health care facilities, providing dialysis services; 4) personal health care institutions because they are entitled to collect consents of persons (granting, withdrawal) that their tissues, cells, organs after their death or live to be collected and used for transplantation; 5) data of persons who granted or withdrew consents that their tissues, cells, organs after their death or live to be collected and used for transplantation. The persons whose data and other relevant information are stored in the Register have a right of access to data and information about himself (herself). The data subject shall, in accordance with the procedure laid down in the Law and the receipt of the documents supporting the facts, have the right to require the Register to correct incorrect, inaccurate, incomplete, eliminate unnecessary or illegally collected data. The Register should provide asked data and information in 5 working days. *3. The State Data Protection Inspectorate of the Republic of Lithuania* According to Article 25 part 1 of the Law on Legal Protection of Personal Data the data subject shall have the right, upon presenting to the data controller or the data processor a document certifying his identity or upon confirming his identity in accordance with the procedure laid down by legal acts or by means of electronic communications which permit a person's identification, to obtain information on the sources and type of his personal data which have been collected, the purpose of their processing and the data recipients to whom the data are disclosed or were disclosed at least during the past year. As Article 5 Paragraph 3 of the Law on the Rights of Patients and Compensation for

	the Damage to their Health provides that "upon presentation of the documents confirming his identity, shall be entitled to receive information about his state of health, diagnosis, methods of treatment or examination applied in the health care institution or alternatives known to the doctor, potential risks, complications, side effects, prognosis of the treatment and other circumstances that may have an effect on the acceptance or rejection by the patient of the proposed treatment, as well as about the consequences of rejecting the proposed treatment" it means that this information might be given in any time after collection of these data by data controller. On another hand Article 25 Paragraph 1 provides that "the data subject shall have the right, <…> to obtain information on the sources and type of his personal data which have been collected, the purpose of their processing and the data recipients to whom the data are disclosed or were disclosed at least during the past year."
Consent:	Is the system based on an opt-in approach? Is the principle of granular consent applied (with the possibility of preventing access to certain data?)? If yes, in which situations?
	1.*The Ministry of Health of the Republic of Lithuania*: The patient under rule of silence allows to process his/her data, to a specialist of healthcare institution by which he/she is served. When the ESPBI will be installed the healthcare specialist will be able to see some patient health records, except for those with the necessary for emergency medical service or services which are paid by Government. 2. *National Transplant Bureau under the Ministry of Health of the Republic of Lithuania*: The principle of granular consent might be used for the adjustment of the data of recipients. For example, in presence of any person to verify the signature or signatures or in some cases, doctors consultations. In any case a patient every time certifies in writing that, agrees that the data on his health would be collected and handled in the Register. *3. The State Data Protection Inspectorate of the Republic of Lithuania* According to Article 2 paragraph 11 of the Law on Legal Protection of Personal Data the consent shall mean an indication of will give freely by a data subject indicating his/her agreement with the processing of his/her personal data for the purposes known to him/her. The consent with regard to special categories of personal data must be expressed clearly, in a written or equivalent form or any other form giving an unambiguous evidence of the data subject's free will. According to Articles 14 – 18 of the Law on the Rights of Patients and Compensation for the Damage to their Health the mechanism for giving of the consent is described as follows: 1) requirements for giving of the consent for the provision of health care services; 2) procedure of expression of consent for health care; 3) giving of the written form of the patient's consent; 4) giving of the consent in emergency situations.

Withdrawal:	Are patients able to withdraw the consent given to EHR schemes? If yes, what is the relevant procedure to withdraw such consent? What are the consequences?
	1.*The Ministry of Health of the Republic of Lithuania*: There is no any regulation while the information system is not implemented. 2. *National Transplant Bureau under the Ministry of Health of the Republic of Lithuania*: There is no practice. *3. The State Data Protection Inspectorate of the Republic of Lithuania*
Outsourcing processing of data:	Is outsourcing common? Under what circumstances? Where is the data outsourced to? What sort of safeguards are in place?
	1.*The Ministry of Health of the Republic of Lithuania*: There is no practice. 2. *National Transplant Bureau under the Ministry of Health of the Republic of Lithuania* Outsourcing shall be executed on legal basis of agreements. *3. The State Data Protection Inspectorate of the Republic of Lithuania* If data processing services are outsourced the data controller is responsible for data protection issues and data processor is obligated to act according to instructions of the data controller.

2. Cloud Computing, Data Mining and Profiling from both Medical Records (including EHR) and Data not specifically related to medical records.

2.1. Data Protection Issues:

Cloud computing has brought a new dimension to the way data is stored, accessed and processed. Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS), Network as a service (NaaS) are all used by services and organisations that deal with both medical data and non-medical data.

With the development of more advanced and efficient data-mining and data-querying Medical techniques (e.g NoSQL, MapReduce, Hadoop) in conjunction with increased processing power and data storage, mining data has never been more informative, easier, and cost-effective.

Healthcare is a natural sector in which to apply new technologies and methodologies, with particular impacts in epidemiology, public health, health services research, etc.

Data that can lead to the identification of a particular individual and his/her health situation is not limited to medical data *per se,* present on Electronic Health Records, but also to unsuspicious type of information.

There is a growing concern that these schemes may be implemented in manner which does not always respect the patients' confidentiality and basic rights, and in a broader context, the use of this of information may prejudice the individuals concerned.

The ability to track and monitor patients and resources enables a more efficient provision of care but may have an impact on the right to privacy of the individual concerned.

2.2. Questions: Is your legal framework providing for a regulation of Cloud Computing, Data Mining and Profiling? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	*1.The Ministry of Health of the Republic of Lithuania*: There is no separate legislation for telecommunication technologies. All regulation is the same as for any other technical infrastructure. 2. *National Transplant Bureau under the Ministry of Health of the Republic of Lithuania* Conditions of and the procedure for the donation, procurement, testing, processing, preservation, storage, distribution and transplantation of human tissues, cells and organs are laid down in the Register which Regulations are approved by the Government of the Republic of Lithuania. Regulations on the Register regulates purpose of collection of human tissues, cells and organs, objects, rights and obligations of data controllers and data processors, data processing, interconnection with other registers, security of data, disclosure of data and information maintained in the Register, reorganisation and winding up of the Register. *3. The State Data Protection Inspectorate of the Republic of Lithuania* There is no separate legislation for cloud computing. The Law on Electronic Communications is applicable.
Case-law:	-
Other:	-

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Cloud computing:	How is cloud computing regulated in your country? Which security safeguards and standards are mandatory? Are there specific requirements in order to store medical data in the cloud? How are data shared and is the sharing regulated?
	1. The Ministry of Health of the Republic of Lithuania: There is no an information. 2. *National Transplant Bureau under the Ministry of Health of the Republic of Lithuania* Article 7 Part 9 of the Law on the Donation and Transplantation of Human Tissues, Cells and Organs settles that data stored in the Register are confidential and might be disclosed according to the order laid down in the Law and other legislation. *3. The State Data Protection Inspectorate of the Republic of Lithuania* There is no separate legislation for cloud computing. The Law on Electronic Communications is applicable.
Government:	Do governmental programmes exist to allow for increased data-mining of medical records? If yes, what are the purposes of this data mining? Are private entities allowed to access the data? Under what circumstances? What sort of techniques and technologies are being used? To what end? Are data subjects informed of this type of data-mining?
	1. The Ministry of Health of the Republic of Lithuania: No, we have not any practice until the system is not implemented. Statistic data will be accessible for all entities whose have a right to process health data and all controlling and managing organizations. However, we have not any practice until the system is not implemented.

2. National Transplant Bureau under the Ministry of Health of the Republic of Lithuania

Entities who are providing data to the Register are as follows:
1) healthcare institutions, which are providing services of donation, procurement, testing, processing, preservation, storage, distribution and transplantation of human tissues, cells and organs;
2) bio banks;
3) healthcare institutions, which are providing dialysis services;
4) healthcare institutions, which are collecting consents or dissents of the persons for transplantation of tissues, cells and organs of living persons or after his/her death;
5) persons who gave or withdrew consents for transplantation of tissues, cells and organs of living persons or after his/her death;
Register data providers have right of access to their data given to the Register. The person has right to apply to the Register as a data processor to be informed about the processing of his personal data, to have an access to his personal data and to be informed of how they are processed, to request rectification or destruction of his personal data or suspension of further processing of his/her personal data. The data controller must inform the data subject during 5 days after execution of his/her order.
Data shall be transferred according to the requirements settled in the Regulations on the Register as it comply the Law on Legal Protection of Personal Data. Any special measures have not applied.

3. The State Data Protection Inspectorate of the Republic of Lithuania
Article 1, part 6 of the Law on Legal Protection of Personal Data shall not restrict or prohibit free movement of personal data when fulfilling European Union membership commitments of the Republic of Lithuania.

Article 5 Paragraph 2 of this Law states that processing of special categories (health data are sensitive or special category of data) is prohibited in general but there are exceptions listed below:

1) the data subject has given his consent;

2) such processing is necessary for the purposes of employment or civil service while exercising rights and fulfilling obligations of the data controller in the field of labour law in the cases laid down in laws;

3) it is necessary to protect vital interests of the data subject or of any other person, where the data subject is unable to give his consent due to a physical disability or legal incapacity;

4) processing of personal data is carried out for political, philosophical, religious purposes or purposes concerning the trade-unions by a foundation, association or any other non-profit organisation, as part of its activities, on condition that the personal data processed concern solely the members of such organisation or to other persons who regularly participate in such organisation in connection with its purposes. Such personal data may not be disclosed to a third party without the data subject's consent;

5) the personal data have been made public by the data subject;

6) the data are necessary, in the cases laid down in laws, in order to prevent and investigate criminal or other illegal activities;

	7) the data are necessary for a court hearing; 8) it is a legal obligation of the data controller under laws to process such data. Paragraph 3 of the same Article provides that data about a person's health may also be processed for the purposes and in the procedure laid down in Article 10 of the Law on Legal Protection of Personal Data and other laws pertaining to health care. Article 10 of the same Law states that health data (its state, diagnosis, prognosis, treatment, etc.) may be processed by an authorised health care professional. A person's health shall be subject to professional secrecy under the Civil Code, laws regulating patients' rights and other legal acts. Personal data processing for scientific medical research purposes shall be carried out in accordance with this and other laws. Personal data on a person's health may be processed by automatic means, also for scientific medical research purposes the data may be processed only having notified the State Data Protection Inspectorate. In this case, the State Data Protection Inspectorate must carry out a prior checking.
Private sector:	Are private entities allowed to mine medical data which they process? Under what circumstances? Can the government have access to this data?
	1. The Ministry of Health of the Republic of Lithuania: Statistical data would be accessible for all entities whose have a right to process health data. No, we have not any practice until the system is not implemented. *2. National Transplant Bureau under the Ministry of Health of the Republic of Lithuania* Entities who are providing data to the Register are as follows: 1) healthcare institutions, which are providing services of donation, procurement, testing, processing, preservation, storage, distribution and transplantation of human tissues, cells and organs; 2) bio banks; 3) healthcare institutions, which are providing dialysis services; 4) healthcare institutions, which are collecting consents or dissents of the persons for transplantation of tissues, cells and organs of living persons or after his/her death; 5) persons who gave or withdrew consents for transplantation of tissues, cells and organs of living persons or after his/her death; Register data providers have right of access to their data given to the Register. The person has right to apply to the Register as a data processor to be informed about the processing of his personal data, to have an access to his personal data and to be informed of how they are processed, to request rectification or destruction of his personal data or suspension of further processing of his/her personal data. The data controller must inform the data subject during 5 days after execution of his/her order. Data shall be transferred according to the requirements settled in the Regulations on the Register as it comply the Law on Legal Protection of Personal Data. *3. The State Data Protection Inspectorate of the Republic of Lithuania* The same approach for governmental and private sectors is applicable and the answer is written above.

Profiling:	Are the government and the private sector allowed to employ profiling methods on medical data? If yes, under what circumstances? Is it allowed to cross and correlate non-medical data with medical data?
	1.The Ministry of Health of the Republic of Lithuania: Functionality of the Information system is under construction and there is no possibility to regulate it yet. Clarification will be made in year 2015. 2. *National Transplant Bureau under the Ministry of Health of the Republic of Lithuania* No, there is no possibility to employ profiling. *3. The State Data Protection Inspectorate of the Republic of Lithuania* Profiling is not regulated in Lithuania. Any definition of it does not exist in National laws. In practice medical data are correlated with non-medical, for example, with health insurance, social security data end etc.

3. RFID and wireless communication technologies

3.1. Data Protection Issues: It is common for medical devices, such as patients' tags, to possess RFID technologies in order to facilitate the transmission of the patients' data. It can also be related to the data-mining operations previously mentioned as it is another category of information that can be used to discern meaningful patterns. Transmission of data through radio-frequency is not limited to medical devices. Almost any smartphone uses some technology enabling to collect, and share, the user's data. For instance, via WI-FI it is possible to identify users' locations and therefore infer some of their behaviour, which in some cases can relate to health information.	
3.2. Questions: Is your legal framework providing for a regulation of RFID technologies and the transfer of personal data through wireless technologies? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	*1.The Ministry of Health of the Republic of Lithuania*: Functionality of the Information system is under construction and there is no possibility to regulate it yet. Data and all information should be transmitted in secure, an encrypted communications channel. The order of the Minister of Health determines model of the architecture of the information system and functional hardware. 2. *National Transplant Bureau under the Ministry of Health of the Republic of Lithuania* The issue is not according to the competency of National Transplant Bureau under the Ministry of Health of the Republic of Lithuania. *3. The State Data Protection Inspectorate of the Republic of Lithuania* There is no separate legislation for RFID. Personal data protection issues are

	regulated by the Law on Electronic Communications and the Law on Legal Protection of Personal Data.
Case-law:	-
Other:	-

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
RFID:	How is RFID used in hospital/clinics for (a) resource management, (b) patient care? What types of database systems (and security) are implemented in conjunction with RFID use? How are issues of access, sharing, consent etc. managed considering that RFID may be used without the patients' knowledge.
	1.The Ministry of Health of the Republic of Lithuania: - 2. *National Transplant Bureau under the Ministry of Health of the Republic of Lithuania* The issue is not according to the competency of National Transplant Bureau under the Ministry of Health of the Republic of Lithuania. *3. The State Data Protection Inspectorate of the Republic of Lithuania* Only soft law is applicable for regulation of RFID. In health care sector RFID is used for marking of samples taken directly from persons or via healthcare institutions, collected for treatment, given to bio banks, transplantation or etc. Personal data protection issues as regards RFID are regulated by the Law on Electronic Communications and the Law on Legal Protection of Personal Data. Also the State Data Protection Inspectorate issued recommendations.
Wireless tracking technologies:	Are hospitals/clinics employing other wireless tracking technologies besides RFID? Which ones? Do they have to follow specific security requirements? Which ones?
	1.The Ministry of Health of the Republic of Lithuania: ___ 2. *National Transplant Bureau under the Ministry of Health of the Republic of Lithuania* The issue is not according to the competency of National Transplant Bureau under the Ministry of Health of the Republic of Lithuania. *3. The State Data Protection Inspectorate of the Republic of Lithuania*

4. Applications (Mobile)

4.1. Data Protection Issues: Information society is increasingly relying on the use of “apps” (application), most of them mobile. These apps are commonly designed to gather personal data, and in practice often process medical data. Technologies such as multi-touch touchscreen, accelerometers or gyroscopes, ambient light sensors, GPS and cameras, and devices featuring fingerprint and biometric sensors also involve the collection of medical data. A mobile phone application can monitor accurately physiological data, such as heartbeats, sleep patterns, fitness information.

4.2. Questions: Is your legal framework providing for a regulation of Apps and Mobile Apps? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs’ opinions and/or case law.	
Legislation:	*1.The Ministry of Health of the Republic of Lithuania*: Apps is not used by health care bodies. Functionality of the Information system is under construction and there is no possibility to regulate it yet. Data and all information should be transmitted in secure, an encrypted communications channel. 2. *National Transplant Bureau under the Ministry of Health of the Republic of Lithuania* The issue is not according to the competency of National Transplant Bureau under the Ministry of Health of the Republic of Lithuania. *3. The State Data Protection Inspectorate of the Republic of Lithuania* *There is no separate legislation for RFID. Personal data protection issues are regulated by the Law on Electronic Communications of the Republic of Lithuania and the Law on Legal Protection of Personal Data of the Republic of Lithuania.*
Case-law:	-
Other:	-

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs’ opinions and/or case law).	
Apps:	Is it allowed to use apps and mobile apps to deploy medical services and collect medical data? If yes, which type of individual/organisation can develop and employ these apps? Are there specific security requirements for these types of apps?
	1.The Ministry of Health of the Republic of Lithuania:

	— 2. *National Transplant Bureau under the Ministry of Health of the Republic of Lithuania* The issue is not according to the competency of National Transplant Bureau under the Ministry of Health of the Republic of Lithuania. *3. The State Data Protection Inspectorate of the Republic of Lithuania* —
Institutions:	Do hospitals/clinics/labs employ apps to gather medical data? Is there a need for a medical treatment to permit the use of an app to process the medical data? Are there specific security requirements for the institutions collecting these data from the apps? Are medico-administrative data used by hospitals/clinics for management purposes?
	1.The Ministry of Health of the Republic of Lithuania: — 2. *National Transplant Bureau under the Ministry of Health of the Republic of Lithuania* There is no according to the competency of National Transplant Bureau under the Ministry of Health of the Republic of Lithuania. *3. The State Data Protection Inspectorate of the Republic of Lithuania* —
Tracking technologies:	Do hospitals/clinics/labs employ non-medical apps and devices to track and collect data from their patients? What type of data is collected? For what purpose? Is the data identifiable? Is the data combined with medical data?
	1.The Ministry of Health of the Republic of Lithuania: — 2. *National Transplant Bureau under the Ministry of Health of the Republic of Lithuania* There is not the competence of National Transplant Bureau under the Ministry of Health of the Republic of Lithuania. *3. The State Data Protection Inspectorate of the Republic of Lithuania* General requirements for organizational and technical data protection measures No 1T-71 approved by the Director of the State Data Protection Inspectorate on 12.11.2008 shall be implemented.
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical apps and tracking apps? If yes, what are the standards?
	1.The Ministry of Health of the Republic of Lithuania: 2. *National Transplant Bureau under the Ministry of Health of the Republic of Lithuania* There is no according to the competency of National Transplant Bureau under the Ministry of Health of the Republic of Lithuania. *3. The State Data Protection Inspectorate of the Republic of Lithuania* General requirements for organizational and technical data protection measures No 1T-71 approved by the Director of the State Data Protection Inspectorate on

	12.11.2008 shall be implemented.
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical diagnostic? How would this be applied to fitness and daily-basis data?
	1.The Ministry of Health of the Republic of Lithuania: A question of use of Medical devices might be included to the future agenda. 2. *National Transplant Bureau under the Ministry of Health of the Republic of Lithuania* There is no according to the competency of National Transplant Bureau under the Ministry of Health of the Republic of Lithuania. *3. The State Data Protection Inspectorate of the Republic of Lithuania* The consent to be given for procedures with any medical devices in the same manner as for treatment plan. According to Article 2 Paragraph 11 of the Law on Legal Protection of Personal Data the consent shall be given freely by the data subject indicating his/her agreement with the processing of his/her personal data for the purposes known to him/her. The consent with regard to special categories of personal data must be expressed clearly, in a written or equivalent form or any other form giving an unambiguous evidence of the data subject's free will.

5. Medical Devices and Wearable Devices

5.1. Data Protection Issues:

A medical device can be defined as: 'any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application. Such a device should be intended by the manufacturer for one of a number of defined purposes, one of which is, diagnosis, prevention, monitoring, treatment or alleviation of disease' (Directive 93/42/EEC Article 1:2)

Some eHealth and mHealth devices and apps do not fall in this definition of medical devices, as can also be the case of a software working in combination with a physical device, for instance a smartphone.

5.2. Questions: Is your legal framework providing for a regulation of Medical Devices? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	*1.The Ministry of Health of the Republic of Lithuania*: State Accreditation Service for Supervision of Health Care Activities carry out medical device registration function, the issue of licenses, it is planned to create the Register of medical devices. 2. *National Transplant Bureau under the Ministry of Health of the Republic of Lithuania* There is not a competence of National Transplant Bureau under the Ministry of Health of the Republic of Lithuania. *3. The State Data Protection Inspectorate of the Republic of Lithuania* General requirements for organizational and technical data protection measures

	No 1T-71 approved by the Director of the State Data Protection Inspectorate on 12.11.2008 shall be used.
Case-law:	-
Other:	-

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
eHealth and mHealth:	*1.The Ministry of Health of the Republic of Lithuania*: State Accreditation Service for Supervision of Health Care Activities carry out medical device registration function, the issue of licenses, it is planned to create the Register of medical devices. 2. *National Transplant Bureau under the Ministry of Health of the Republic of Lithuania* There is not competence of National Transplant Bureau under the Ministry of Health of the Republic of Lithuania. *3. The State Data Protection Inspectorate of the Republic of Lithuania* General requirements for organizational and technical data protection measures No 1T-71 approved by the Director of the State Data Protection Inspectorate on 12.11.2008 shall be implemented. _____ Does the concept of Medical device in your country encompass services and apparels in the realm of eHealth and mHealth? What are the requirements? Should, for instance, the medical device be certified before it can be used?
	1.The Ministry of Health of the Republic of Lithuania: State Accreditation Service for Supervision of Health Care Activities is responsible that medical devices shall comply data security requirements. 2. *National Transplant Bureau under the Ministry of Health of the Republic of Lithuania* There is not a competence of National Transplant Bureau under the Ministry of Health of the Republic of Lithuania. *3. The State Data Protection Inspectorate of the Republic of Lithuania* General requirements for organizational and technical data protection measures No 1T-71 approved by the Director of the State Data Protection Inspectorate on 12.11.2008 shall be implemented.
Apps	Does the concept of medical devices encompass apps? If yes, is there any regulation applicable to apps that perform medical services? Is there any regulation applicable on apps that track non-medical data that can lead to health information? If yes, what type of data?
	1.The Ministry of Health of the Republic of Lithuania: Apps is not used for health care services provision. 2. *National Transplant Bureau under the Ministry of Health of the Republic of Lithuania* There is not the competence of National Transplant Bureau under the Ministry of Health of the Republic of Lithuania.

	3. The State Data Protection Inspectorate of the Republic of Lithuania General requirements for organizational and technical data protection measures No 1T-71 approved by the Director of the State Data Protection Inspectorate on 12.11.2008 shall be implemented.
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical and/or wearable devices? If yes, what are the standards?
	1.The Ministry of Health of the Republic of Lithuania: State Accreditation Service for Supervision of Health Care Activities carry out medical device registration function, the issue of licenses, it is planned to create the Register of medical devices. 2. *National Transplant Bureau under the Ministry of Health of the Republic of Lithuania* There is no according to the competency of National Transplant Bureau under the Ministry of Health of the Republic of Lithuania. *3. The State Data Protection Inspectorate of the Republic of Lithuania*
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical treatment? How would this be applied to fitness and daily-basis data?
	1.The Ministry of Health of the Republic of Lithuania: A question of order to use new Medical devices to be included to the future agenda.

6. Internet of Things

6.1. Data Protection Issues:

Internet of things relates to common, ordinary devices that are now, and increasingly, connected to the Internet, such as cars, fridges, ovens, microwaves, etc. All of these devices can provide data that can lead to reveal information concerning one's health. A fridge can easily inform on the type of food stored and thus the diet of an individual. One of the biggest challenges of the Internet of Things is to guarantee the right to privacy and data protection in a world where every device collects, processes, analyses and transmits the data, commonly via wireless technologies.

In the realm of medical data, the issue mainly arises when crossing seemly unrelated data that can lead to health information about an individual.

6.2. Questions: Is your legal framework providing for a regulation of the Internet of Things? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	*1.The Ministry of Health of the Republic of Lithuania*: 2. *National Transplant Bureau under the Ministry of Health of the Republic of Lithuania* There is not the competence of National Transplant Bureau under the Ministry of Health of the Republic of Lithuania.

	3. The State Data Protection Inspectorate of the Republic of Lithuania There are not special legal requirements and sanctions. The recommendations shall be issued in year 2015. General requirements for organizational and technical data protection measures No 1T-71 approved by the Director of the State Data Protection Inspectorate on 12.11.2008 shall be implemented.
Case-law:	-
Other:	-

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Security:	What are the security standards that need to be employed by these devices when collecting personal data?
	1.The Ministry of Health of the Republic of Lithuania: 2. *National Transplant Bureau under the Ministry of Health of the Republic of Lithuania* There is not the competence of National Transplant Bureau under the Ministry of Health of the Republic of Lithuania. *3. The State Data Protection Inspectorate of the Republic of Lithuania* There are not special legal requirements and sanctions. The recommendations shall be issued in year 2015. General requirements for organizational and technical data protection measures No 1T-71 approved by the Director of the State Data Protection Inspectorate on 12.11.2008 shall be implemented.
Non-medical devices:	Are non-medical devices allowed to collect medical data, such as heart frequency? Are they allowed to cross medical data with non-medical data?
	. *1.The Ministry of Health of the Republic of Lithuania*: Non-medical devices for medical purpose do not use any health care institution. 2. *National Transplant Bureau under the Ministry of Health of the Republic of Lithuania* There is not the competence of National Transplant Bureau under the Ministry of Health of the Republic of Lithuania. *3. The State Data Protection Inspectorate of the Republic of Lithuania* There are not special legal requirements and sanctions. The recommendations shall be issued in year 2015. General requirements for organizational and technical data protection measures No 1T-71 approved by the Director of the State Data Protection Inspectorate on 12.11.2008 shall be implemented.
Privacy by Design:	Is there any requirement to implement privacy by design in the development of connected devices? If yes, what are the standards?
	1.The Ministry of Health of the Republic of Lithuania: 2. *National Transplant Bureau under the Ministry of Health of the Republic of Lithuania* There is not the competence of National Transplant Bureau under the Ministry of Health of the Republic of Lithuania. *3. The State Data Protection Inspectorate of the Republic of Lithuania*

	Some preparation for implementation of the principle “privacy by design” already started.

7. Electronic Doctor (online Doctor) and on-line appointments

7.1. Data Protection Issues:

The Doctor listens, talks and assesses the patient online, via a website, app, canal, sometimes including video-conference. Medical data is collected and processed, what are the security requirements and standards followed? Other websites provide for on-line appointments with doctors, which can also involve the processing of medical data.

7.2. Questions: Is your legal framework providing for a regulation of online Medical Treatment and is the on-line appointment system covered by such a framework? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs’ opinions and/or case law.

Legislation:	*1.The Ministry of Health of the Republic of Lithuania*: E-doctor conception is included to the job description of one specialist. It is lack of specialists of tele-services, for example, tele-radiology, tele-cardiology and etc. *2. National Transplant Bureau under the Ministry of Health of the Republic of Lithuania* There is not the competence of National Transplant Bureau under the Ministry of Health of the Republic of Lithuania. *3. The State Data Protection Inspectorate of the Republic of Lithuania* Some preparation for supervision in e-health field already started.
TheCase-law:	-
Other:	-

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs’ opinions and/or case law).	
Medical treatment:	Is it allowed to perform medical treatment via online services? If yes, how should the medical services be provided? Does it have to follow the same requirements of a regular physically-present medical treatment?
	.
Medical data:	How should the data collected via a medical treatment performed online be processed? Are there specific requirements? Which ones?

Other comments and technologies
Should you wish to describe any technology, feature or trend that has not been covered by the questionnaire, please feel free to use the space provided below. Where relevant, also indicate recent legislation changes, guidelines and/or case law.
-

GERMANY / ALLEMAGNE

QUESTIONNAIRE

The questionnaire should ideally be completed by data protection authorities, health policy authorities, professional or patient associations as well as healthcare providers: you are invited to share it as widely as possible.

Please send your replies to dataprotection@coe.int no later than 15 December 2014.

1. Mobile Health (mHealth) and Electronic Health Records (EHR)

1.1. Data Protection Issues:

This is perhaps the biggest topic sitting at the intersection of technology and data protection. Mobile health (mHealth) and Electronic Health Records (EHR) are increasingly used in healthcare systems and provisions – it is a trend that needs to be examined.

Related to the EHR, these records are more accurate, cost-effective (in terms of storage) than paper-based notes. The concept of patient controlled/accessed EHR has been implemented in varying degrees in different countries.

Furthermore, some non-medical record can still contain health information about users and it should be considered if such records ought to be treated in a similar way to EHR.

Also, should 'medical data' as defined in Recommendation N° (97) 5 on the protection of medical data cover physical tracking data, such as pedometers or fitness data and data that can lead to medical information about an individual ?

1.2. Questions: if EHR exist in your country, is your legal framework providing for a regulation of such records? If mHealth exists in your country, is your legal framework providing for a specific regulation? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	In Germany there exist different kinds of EHR with different legal frameworks. One of these is the EHR which is provided by the electronic health card. The legal basis is laid down in §§ 291, 291a SGB V (Book of Social Security). The following comments exclusively concern this kind of EHR. The storing of medical data in this EHR is voluntary for the patient. Patients have to consent to the storage and use of electronic medical data, in particular by technical access authorisation (PIN code), and can withdraw their consent at any time. Additionally, they have the right to access their data in a secured environment. The access of EHR requires an electronic health card in conjunction with a health professional card. Activation and usage of both cards require PIN codes. Furthermore all access to the data is recorded with the 50 most recent accesses being stored. The medical data in EHR may only be used for medical care. As additional legal safeguard, electronic health card data are protected by law against confiscation, non-medical usage and telecommunications data retention. The legal framework was built in close cooperation with the Federal Commissioner for Data Protection.

Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
EHR and Medical data:	What can be considered medical data in your country? Is it solely the data relating to a person's health (state, diagnosis, prognosis, medical treatment, etc.)? Is non-medical data that leads to medical information treated the same way as medical data (for instance in terms of confidentiality requirements)? Is the EHR solely constituted of data collected in a medical context or can the individual also himself or herself add information regarding his or her health?
	There exists no definition for medical data in Germany. But medical data include also data from which the state of health indirectly arises. The patient himself cannot add informations in the EHR. In connection with his own signature card that holds a qualified signature, the patient may, in separate files, also administrate their own data or data supplied to them by their care providers.
Sharing of data and Access:	Who is granted access to the EHR and how is the sharing of information (with other health care providers?) regulated? Where information is shared with pharmacists, is there a strict purpose limitation in place? How has the definition of the responsibility over the medical data been regulated?
	With the consent of the patient, doctors, dentists. pharmacists and psychotherapists have autonomous access to EHR. The access is only legal for the purpose of medical care of the patient.
Data quality:	Are the principles of legitimacy, fairness and minimisation applied to medical data? How are records kept accurate? How long is the data kept for, is the specific storage period defined for the EHR?
	For the storing of medical data the common data protection rules apply. They contain legitimacy, fairness and minimization.
Data integrity:	Are any specific methods used to ensure the integrity of the data? How are patients identified in the EHR? In the context of research, are anonymisation methods used and what safeguards exist for re-identification?
	The electronic health card for patients contains means for electronic authorisation. Doctors, dentists, pharmacists and psychotherapists can access sensitive health data on EHR provided by electronic health card only via an encrypted communication route. They have to identify themselves to the system with strict security using their electronic Health Professional Card.
Data security:	Where are the records stored? Is there a centralised database of EHR? What security technology is being used?
	The EHR is stored on several servers which are then accessed by means of electronic references held on the card.

Rights of the person/patient concerned:	How can the right of access be exercised? How can the data be corrected? Can the person enter information in his or her own EHR? What are the legal remedies available?
	Patients can look at the data stored on their electronic health card in a secured environment and obtain printouts. The right to access the data is regulated by law. The patient cannot enter information in his EHR himself. In connection with their own signature card that holds a qualified signature, patients may, in separate files, also administrate their own data or data supplied to them by their care providers.
Consent:	Is the system based on an opt-in approach? Is the principle of granular consent applied (with the possibility of preventing access to certain data?)? If yes, in which situations?
	Yes, the system is based on an opt-in approach. The health data component of the card is intended to be used only on a voluntary basis. This means that every patient will be free to decide whether or not they want to make use of storing medical data in the EHR. Consent can be limited to certain data. The patients can decide whether or not and which of their health data are to be stored or deleted and who is entitled to access these data.
Withdrawal:	Are patients able to withdraw the consent given to EHR schemes? If yes, what is the relevant procedure to withdraw such consent? What are the consequences?
	The patient has the right to withdraw the consent at any time. He has to withdraw the consent in writing. He has the right to deletion of the data of EHR.
Outsourcing processing of data:	Is outsourcing common? Under what circumstances? Where is the data outsourced to? What sort of safeguards are in place?
	The EHR which is provided by the electronic health card is stored on several servers which are then accessed by means of electronic references held on the card.

2. Cloud Computing, Data Mining and Profiling from both Medical Records (including EHR) and Data not specifically related to medical records.

2.1. Data Protection Issues:

Cloud computing has brought a new dimension to the way data is stored, accessed and processed. Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS), Network as a service (NaaS) are all used by services and organisations that deal with both medical data and non-medical data.

With the development of more advanced and efficient data-mining and data-querying Medical techniques (e.g NoSQL, MapReduce, Hadoop) in conjunction with increased processing power and data storage, mining data has never been more informative, easier, and cost-effective.

Healthcare is a natural sector in which to apply new technologies and methodologies, with particular impacts in epidemiology, public health, health services research, etc.

Data that can lead to the identification of a particular individual and his/her health situation is not

limited to medical data *per se,* present on Electronic Health Records, but also to unsuspicious type of information.

There is a growing concern that these schemes may be implemented in manner which does not always respect the patients' confidentiality and basic rights, and in a broader context, the use of this of information may prejudice the individuals concerned.

The ability to track and monitor patients and resources enables a more efficient provision of care but may have an impact on the right to privacy of the individual concerned.

2.2. Questions: Is your legal framework providing for a regulation of Cloud Computing, Data Mining and Profiling? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Cloud computing:	How is cloud computing regulated in your country? Which security safeguards and standards are mandatory? Are there specific requirements in order to store medical data in the cloud? How is data shared and is the sharing regulated?
Government:	Do governmental programmes exist to allow for increased data-mining of medical records? If yes, what are the purposes of this data mining? Are private entities allowed to access the data? Under what circumstances? What sort of techniques and technologies are being used? To what end? Are data subjects informed of this type of data-mining?
Private sector:	Are private entities allowed to mine medical data which they process? Under what circumstances? Can the government have access to this data?
Profiling:	Are the government and the private sector allowed to employ profiling methods on medical data? If yes, under what circumstances? Is it allowed to cross and correlate non-medical data with medical data?

3. RFID and wireless communication technologies

3.1. Data Protection Issues:

It is common for medical devices, such as patients' tags, to possess RFID technologies in order to facilitate the transmission of the patients' data.

It can also be related to the data-mining operations previously mentioned as it is another category of information that can be used to discern meaningful patterns.

Transmission of data through radio-frequency is not limited to medical devices. Almost any

smartphone uses some technology enabling to collect, and share, the user's data. For instance, via WI-FI it is possible to identify users' locations and therefore infer some of their behaviour, which in some cases can relate to health information.

3.2. Questions: Is your legal framework providing for a regulation of RFID technologies and the transfer of personal data through wireless technologies? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
RFID:	How is RFID used in hospital/clinics for (a) resource management, (b) patient care? What types of database systems (and security) are implemented in conjunction with RFID use? How are issues of access, sharing, consent etc. managed considering that RFID may be used without the patients' knowledge.
Wireless tracking technologies:	Are hospitals/clinics employing other wireless tracking technologies besides RFID? Which ones? Do they have to follow specific security requirements? Which ones?

4. Applications (Mobile)

4.1. Data Protection Issues:
Information society is increasingly relying on the use of "apps" (application), most of them mobile. These apps are commonly designed to gather personal data, and in practice often process medical data. Technologies such as multi-touch touchscreen, accelerometers or gyroscopes, ambient light sensors, GPS and cameras, and devices featuring fingerprint and biometric sensors also involve the collection of medical data. A mobile phone application can monitor accurately physiological data, such as heartbeats, sleep patterns, fitness information.

4.2. Questions: Is your legal framework providing for a regulation of Apps and Mobile Apps? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Apps:	Is it allowed to use apps and mobile apps to deploy medical services and collect medical data? If yes, which type of individual/organisation can develop and employ

	these apps? Are there specific security requirements for these types of apps?
Institutions:	Do hospitals/clinics/labs employ apps to gather medical data? Is there a need for a medical treatment to permit the use of an app to process the medical data? Are there specific security requirements for the institutions collecting these data from the apps? Are medico-administrative data used by hospitals/clinics for management purposes?
Tracking technologies:	Do hospitals/clinics/labs employ non-medical apps and devices to track and collect data from their patients? What type of data is collected? For what purpose? Is the data identifiable? Is the data combined with medical data?
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical apps and tracking apps? If yes, what are the standards?
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical diagnostic? How would this be applied to fitness and daily-basis data?

5. Medical Devices and Wearable Devices

5.1. Data Protection Issues:

A medical device can be defined as: 'any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application. Such a device should be intended by the manufacturer for one of a number of defined purposes, one of which is, diagnosis, prevention, monitoring, treatment or alleviation of disease' (Directive 93/42/EEC Article 1:2)

Some eHealth and mHealth devices and apps do not fall in this definition of medical devices, as can also be the case of a software working in combination with a physical device, for instance a smartphone.

5.2. Questions: Is your legal framework providing for a regulation of Medical Devices? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
eHealth and mHealth:	Does the concept of Medical device in your country encompass services and apparels in the realm of eHealth and mHealth? What are the requirements?

	Should, for instance, the medical device be certified before it can be used?
Apps:	Does the concept of medical devices encompass apps? If yes, is there any regulation applicable to apps that perform medical services? Is there any regulation applicable on apps that track non-medical data that can lead to health information? If yes, what type of data?
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical and/or wearable devices? If yes, what are the standards?
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical treatment? How would this be applied to fitness and daily-basis data?

6. Internet of Things

6.1. Data Protection Issues:

Internet of things relates to common, ordinary devices that are now, and increasingly, connected to the Internet, such as cars, fridges, ovens, microwaves, etc. All of these devices can provide data that can lead to reveal information concerning one's health. A fridge can easily inform on the type of food stored and thus the diet of an individual. One of the biggest challenges of the Internet of Things is to guarantee the right to privacy and data protection in a world where every device collects, processes, analyses and transmits the data, commonly via wireless technologies.

In the realm of medical data, the issue mainly arises when crossing seemly unrelated data that can lead to health information about an individual.

6.2. Questions: Is your legal framework providing for a regulation of the Internet of Things? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Security:	What are the security standards that need to be employed by these devices when collecting personal data?
Non-medical devices:	Are non-medical devices allowed to collect medical data, such as heart frequency? Are they allowed to cross medical data with non-medical data?

Privacy by Design:	Is there any requirement to implement privacy by design in the development of connected devices? If yes, what are the standards?

7. Electronic Doctor (online Doctor) and on-line appointments

7.1. Data Protection Issues:

The Doctor listens, talks and assesses the patient online, via a website, app, canal, sometimes including video-conference. Medical data is collected and processed, what are the security requirements and standards followed? Other websites provide for on-line appointments with doctors, which can also involve the processing of medical data.

7.2. Questions: Is your legal framework providing for a regulation of online Medical Treatment and is the on-line appointment system covered by such a framework? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	.
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Medical treatment:	Is it allowed to perform medical treatment via online services? If yes, how should the medical services be provided? Does it have to follow the same requirements of a regular physically-present medical treatment?
	The professional code of conduct (Musterberufsordnung) for german doctors states, that doctors are not allowed to medical treatment only through print and communications media. In Germany, therefore, there is no absolute ban on remote treatment, but a ban on the exclusive remote treatment.
Medical data:	How should the data collected via a medical treatment performed online be processed? Are there specific requirements? Which ones?

Other comments and technologies
Should you wish to describe any technology, feature or trend that has not been covered by the questionnaire, please feel free to use the space provided below. Where relevant, also indicate recent legislation changes, guidelines and/or case law.

HUNGARY / HONGRIE

QUESTIONNAIRE

The questionnaire should ideally be completed by data protection authorities, health policy authorities, professional or patient associations as well as healthcare providers: you are invited to share it as widely as possible.

Please send your replies to dataprotection@coe.int no later than 15 December 2014.

1. Mobile Health (mHealth) and Electronic Health Records (EHR)

1.1. Data Protection Issues:

This is perhaps the biggest topic sitting at the intersection of technology and data protection. Mobile health (mHealth) and Electronic Health Records (EHR) are increasingly used in healthcare systems and provisions – it is a trend that needs to be examined.

Related to the EHR, these records are more accurate, cost-effective (in terms of storage) than paper-based notes. The concept of patient controlled/accessed EHR has been implemented in varying degrees in different countries.

Furthermore, some non-medical record can still contain health information about users and it should be considered if such records ought to be treated in a similar way to EHR.

Also, should 'medical data' as defined in Recommendation N° (97) 5 on the protection of medical data cover physical tracking data, such as pedometers or fitness data and data that can lead to medical information about an individual ?

1.2. Questions: if EHR exist in your country, is your legal framework providing for a regulation of such records? If mHealth exists in your country, is your legal framework providing for a specific regulation? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	
Case-law:	
Other:	*The regulation of health data protection is technology independent in Hungary. This means that there is no specific regulation either for electronic vs. paper based health records nor for different electronic devices that can carry the health information*

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
EHR and Medical data:	What can be considered medical data in your country? Is it solely the data relating to a person's health (state, diagnosis, prognosis, medical treatment, etc.)? Is non-medical data that leads to medical information treated the same way as medical data (for instance in terms of confidentiality requirements)? Is the EHR solely constituted of data collected in a medical context or can the individual also himself or herself add information regarding his or her health?

	Any information that refers to physical, mental, psychological status, addictions, illnesses, circumstances and causes of death of a person is considered as health information (Law of Health Data Protection ACT 47/1997) *It is not customary in Hungary that patients themselves add information to their health records. Health records usually organised in an episode based approach, each record contains information in context of a given treatment episode. In other words, there is no life-long health record in Hungary.*
Sharing of data and Access:	Who is granted access to the EHR and how is the sharing of information (with other health care providers?) regulated? Where information is shared with pharmacists, is there a strict purpose limitation in place? How has the definition of the responsibility over the medical data been regulated?
	As a general principle, general practitioners are authorised to access all health information of their patients. In secondary care e.g. in a hospital only those physicians have the right to access patient data who are directly involved in the treatment o the patient. *Generally health data are not shared with pharmacist, other than is written in the prescription. In some cases ICD codes appear on prescriptions.*
Data quality:	Are the principles of legitimacy, fairness and minimisation applied to medical data? How are records kept accurate? How long is the data kept for, is the specific storage period defined for the EHR?
	The quality of health data is entirely in the responsibility of the physicians. *The data typically should be preserved for 30 years, discharge reports for 50 years, images, prescriptions for 5 years.* *There is no different rules for electronic data, except that it is necessary to ensure, that the device that carries electronic data remains readable, so the data are sensibly accessible.*
Data integrity:	Are any specific methods used to ensure the integrity of the data? How are patients identified in the EHR? In the context of research, are anonymisation methods used and what safeguards exist for re-identification?
	Patients are identified by natural identifiers (name, birth data etc.) and social insurance identifier (TAJ) This applies both for electronic and paper based data. Certain reports (e.g. reimbursement claim reports) does not contain natural identifiers. *Data that contains personal identifiers can be used for research purposes under specific regulations, and publication of results of such a research cannot contain any information that makes patients recognisable. Anonymous (or pseudonym) data are not considered as personal, but no data can be published if there is not at least three individuals behind each data elements.*
Data security:	Where are the records stored? Is there a centralised database of EHR? What security technology is being used?
	Until now there was no specific regulation on data protection technology. *According to a new regulation each information system should be classified according to sensitivity into five security level, and there different security measures should be applied at each level.* *There is no central EHR repository up to now in Hungary. Record storage is under the responsibility of the institute where data were originally recorded. This can be inside the institute, or at a contracted server hosting service provider.*

	Storage in health data in cloud is not accepted, however regulation is not quite clear.
Rights of the person/patient concerned:	How can the right of access be exercised? How can the data be corrected? Can the person enter information in his or her own EHR? What are the legal remedies available?
	The patient and relatives (authorized by the patient) has the right to access all medical record, and request extra copies on his or her expense. (Only technical costs can be charged, the information itself is free). In case of error the patient has the right to warn the physician, but final decision and responsibility remains at the physician. If the patient and the physician disagree, the patient can turn to the "commissioner of patient rights". Such a commissioner works at each hospital. *Again there is no difference between EHR and paper based records.*
Consent:	Is the system based on an opt-in approach? Is the principle of granular consent applied (with the possibility of preventing access to certain data?)? If yes, in which situations?
	All access to personal health data must be based on written permission of the patient, except those that are explicitly declared in law. The granular consent principle is not directly mentioned in the law, but can be inferred. However it is a technical challenge in the new EHR systems that are currently developed. It is possible that especially sensitive data e.g. psychiatric data will be managed differently
Withdrawal:	Are patients able to withdraw the consent given to EHR schemes? If yes, what is the relevant procedure to withdraw such consent? What are the consequences?
	In principle withdraw is possible, but does not happen commonly.
Outsourcing processing of data:	Is outsourcing common? Under what circumstances? Where is the data outsourced to? What sort of safeguards are in place?
	Outsourcing is not common but not forbidden. The data protection law discriminates data handler (a person or body that is legally authorized and responsible for managing data) and data processing actor who manages the data technically under a written contract of the data handler. Safeguards should be written in the contract, it is the responsibility of the data handler

2. Cloud Computing, Data Mining and Profiling from both Medical Records (including EHR) and Data not specifically related to medical records.

2.1. Data Protection Issues:

Cloud computing has brought a new dimension to the way data is stored, accessed and processed. Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS), Network as a service (NaaS) are all used by services and organisations that deal with both medical data and non-medical data.

With the development of more advanced and efficient data-mining and data-querying Medical techniques (e.g NoSQL, MapReduce, Hadoop) in conjunction with increased processing power and data storage, mining data has never been more informative, easier, and cost-effective.

Healthcare is a natural sector in which to apply new technologies and methodologies, with particular impacts in epidemiology, public health, health services research, etc. Data that can lead to the identification of a particular individual and his/her health situation is not limited to medical data *per se,* present on Electronic Health Records, but also to unsuspicious type of information. There is a growing concern that these schemes may be implemented in manner which does not always respect the patients' confidentiality and basic rights, and in a broader context, the use of this of information may prejudice the individuals concerned. The ability to track and monitor patients and resources enables a more efficient provision of care but may have an impact on the right to privacy of the individual concerned.

2.2. Questions: Is your legal framework providing for a regulation of Cloud Computing, Data Mining and Profiling? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	
Case-law:	
Other:	*There is no specific legislation for cloud computing. Use of health data for research purposes is regulated in the Law of Health Data Protection, this applies for data mining also.*

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Cloud computing:	How is cloud computing regulated in your country? Which security safeguards and standards are mandatory? Are there specific requirements in order to store medical data in the cloud? How is data shared and is the sharing regulated?
	See the remark above.
Government:	Do governmental programmes exist to allow for increased data-mining of medical records? If yes, what are the purposes of this data mining? Are private entities allowed to access the data? Under what circumstances? What sort of techniques and technologies are being used? To what end? Are data subjects informed of this type of data-mining?
	Such programmes does not exist. Any research on health data can be carried out in personal or in anonymous form. Personal research – if it is carried out by an actor otherwise not authorized – can be done only after ethical approval and written consent of the patient. Anonymous or pseudonymous data can be used for research, but guarantee should be given to avoid re-personalisation.
Private sector:	Are private entities allowed to mine medical data which they process? Under what circumstances? Can the government have access to this data?
	Companies that manage health data under a contract with the responsible data handler are not allowed to mine medical data. Their contract bind them to secrecy.
Profiling:	Are the government and the private sector allowed to employ profiling methods on medical data? If yes, under what circumstances? Is it allowed to cross and correlate non-medical data with medical data?

	Only if individuals cannot be identified

3. RFID and wireless communication technologies

3.1. Data Protection Issues:

It is common for medical devices, such as patients' tags, to possess RFID technologies in order to facilitate the transmission of the patients' data.

It can also be related to the data-mining operations previously mentioned as it is another category of information that can be used to discern meaningful patterns.

Transmission of data through radio-frequency is not limited to medical devices. Almost any smartphone uses some technology enabling to collect, and share, the user's data. For instance, via WI-FI it is possible to identify users' locations and therefore infer some of their behaviour, which in some cases can relate to health information.

3.2. Questions: Is your legal framework providing for a regulation of RFID technologies and the transfer of personal data through wireless technologies? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	
Case-law:	
Other:	*There is no specific regulation on RFID-s and wireless devices. Data protection legislation is technology independent.*

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
RFID:	How is RFID used in hospital/clinics for (a) resource management, (b) patient care? What types of database systems (and security) are implemented in conjunction with RFID use? How are issues of access, sharing, consent etc. managed considering that RFID may be used without the patients' knowledge.
	RFID-s are used rarely and – according to my knowledge – only for resource management.
Wireless tracking technologies:	Are hospitals/clinics employing other wireless tracking technologies besides RFID? Which ones? Do they have to follow specific security requirements? Which ones?
	Not known

4. Applications (Mobile)

4.1. Data Protection Issues:

Information society is increasingly relying on the use of "apps" (application), most of them mobile. These apps are commonly designed to gather personal data, and in practice often process medical data.
Technologies such as multi-touch touchscreen, accelerometers or gyroscopes, ambient light sensors,

GPS and cameras, and devices featuring fingerprint and biometric sensors also involve the collection of medical data. A mobile phone application can monitor accurately physiological data, such as heartbeats, sleep patterns, fitness information.

4.2. Questions: Is your legal framework providing for a regulation of Apps and Mobile Apps? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	
Case-law:	
Other:	*Again, legislation is technology independent*

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Apps:	Is it allowed to use apps and mobile apps to deploy medical services and collect medical data? If yes, which type of individual/organisation can develop and employ these apps? Are there specific security requirements for these types of apps?
	There are experimental cases (telemedicine, home monitoring) Such data collections are allowed if the system meets all legal requirements and technically ensure privacy. However the necessary security level is not yet specified..
Institutions:	Do hospitals/clinics/labs employ apps to gather medical data? Is there a need for a medical treatment to permit the use of an app to process the medical data? Are there specific security requirements for the institutions collecting these data from the apps? Are medico-administrative data used by hospitals/clinics for management purposes?
	Not known
Tracking technologies:	Do hospitals/clinics/labs employ non-medical apps and devices to track and collect data from their patients? What type of data is collected? For what purpose? Is the data identifiable? Is the data combined with medical data?
	Not known
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical apps and tracking apps? If yes, what are the standards?
	Again, the law is technology independent, standards are not yet applied legally.
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical diagnostic? How would this be applied to fitness and daily-basis data?
	Only voluntary patients are involved

5. Medical Devices and Wearable Devices

5.1. Data Protection Issues: A medical device can be defined as: 'any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application. Such a device should be intended by the manufacturer for one of a number of defined purposes, one of which is, diagnosis, prevention, monitoring, treatment or alleviation of disease' (Directive 93/42/EEC Article 1:2) Some eHealth and mHealth devices and apps do not fall in this definition of medical devices, as can also be the case of a software working in combination with a physical device, for instance a smartphone.

5.2. Questions: Is your legal framework providing for a regulation of Medical Devices? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	*The legal framework for medical devices (4/2009. (III. 17.) EüM rendelet) and data protection (Law of Health Data Protection ACT 47/1997) are independent.* *Legislation on medical devices focuses on patient safety, while all privacy issues are dealt with in the Law of Health Data protection)*
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
eHealth and mHealth:	Does the concept of Medical device in your country encompass services and apparels in the realm of eHealth and mHealth? What are the requirements? Should, for instance, the medical device be certified before it can be used?
	In principle all medical devices have to be certified according to the EU regulation. According to our knowledge special legislation and specific certification procedure does not exist for mHealth
Apps:	Does the concept of medical devices encompass apps? If yes, is there any regulation applicable to apps that perform medical services? Is there any regulation applicable on apps that track non-medical data that can lead to health information? If yes, what type of data?
	In principle yes, the same as for all medical software. However we do not know cases of medical software certification procedure that is specifically related to data protection issues. *Use of non-medical data is regulated by the general data protection law (Law on information self-determination and on freedom of information ACT 112/2011) The law does not mention specific non-medical data that might lead to health information.*
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical and/or wearable devices? If yes, what are the standards?
	Specific standards are not known
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical treatment? How would this be applied to fitness and daily-basis data?
	Consent requirements also technology independent. The patient must be warned to all known possible risk of any medical treatment, written consensus is necessary

	for surgical procedures. Use of personal data also requires written consensus except cases where specific law authorises. This applies for automated data collection by (wearable) medical devices also.

6. Internet of Things

6.1. Data Protection Issues:

Internet of things relates to common, ordinary devices that are now, and increasingly, connected to the Internet, such as cars, fridges, ovens, microwaves, etc. All of these devices can provide data that can lead to reveal information concerning one's health. A fridge can easily inform on the type of food stored and thus the diet of an individual. One of the biggest challenges of the Internet of Things is to guarantee the right to privacy and data protection in a world where every device collects, processes, analyses and transmits the data, commonly via wireless technologies.

In the realm of medical data, the issue mainly arises when crossing seemly unrelated data that can lead to health information about an individual.

6.2. Questions: Is your legal framework providing for a regulation of the Internet of Things? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	
Case-law:	
Other:	*The notion of "internet of things" does not appear in Hungarian legislation*

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Security:	What are the security standards that need to be employed by these devices when collecting personal data?
	-
Non-medical devices:	Are non-medical devices allowed to collect medical data, such as heart frequency? Are they allowed to cross medical data with non-medical data?
	-
Privacy by Design:	Is there any requirement to implement privacy by design in the development of connected devices? If yes, what are the standards?
	-

7. Electronic Doctor (online Doctor) and on-line appointments

7.1. Data Protection Issues:

The Doctor listens, talks and assesses the patient online, via a website, app, canal, sometimes including video-conference. Medical data is collected and processed, what are the security requirements and standards followed? Other websites provide for on-line appointments with doctors,

which can also involve the processing of medical data.

7.2. Questions: Is your legal framework providing for a regulation of online Medical Treatment and is the on-line appointment system covered by such a framework? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	
Case-law:	
Other:	*Treatment is generally carried out and financed on direct patient – physician contact episodes. Such episodes can however extended by remote communication, either by traditional ways, such as telephone calls, or by submission of data by any means.*

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Medical treatment:	Is it allowed to perform medical treatment via online services? If yes, how should the medical services be provided? Does it have to follow the same requirements of a regular physically-present medical treatment?
	According to our best knowledge this does not happen in Hungary, since all reimbursement is based on direct contact.
Medical data:	How should the data collected via a medical treatment performed online be processed? Are there specific requirements? Which ones?
	-

Other comments and technologies
Should you wish to describe any technology, feature or trend that has not been covered by the questionnaire, please feel free to use the space provided below. Where relevant, also indicate recent legislation changes, guidelines and/or case law.
As mentioned above, the general rule is that legislation does not deal with specific technologies. As technology changes rapidly, it seems to be reasonable. Legislation defines the rights to collect, store, process and transmit data. The necessary technical means to ensure safety and privacy is under the responsibility of the actors, however in case of accusation the data handler has to prove that he made all reasonable measures. *This situation is changing somehow now however by the fact that according to a new legislation all information systems have to be classified according to the sensitivity of handled data and risk of infringement. The legislation specifies the level of minimum technical security for each sensitivity class.*

ICELAND / ISLANDE

QUESTIONNAIRE

The questionnaire should ideally be completed by data protection authorities, health policy authorities, professional or patient associations as well as healthcare providers: you are invited to share it as widely as possible.

Please send your replies to dataprotection@coe.int no later than 15 December 2014.

1. Mobile Health (mHealth) and Electronic Health Records (EHR)

1.1. Data Protection Issues:

This is perhaps the biggest topic sitting at the intersection of technology and data protection. Mobile health (mHealth) and Electronic Health Records (EHR) are increasingly used in healthcare systems and provisions – it is a trend that needs to be examined.

Related to the EHR, these records are more accurate, cost-effective (in terms of storage) than paper-based notes. The concept of patient controlled/accessed EHR has been implemented in varying degrees in different countries.

Furthermore, some non-medical record can still contain health information about users and it should be considered if such records ought to be treated in a similar way to EHR.

Also, should 'medical data' as defined in Recommendation N° (97) 5 on the protection of medical data cover physical tracking data, such as pedometers or fitness data and data that can lead to medical information about an individual ?

1.2. Questions: if EHR exist in your country, is your legal framework providing for a regulation of such records? If mHealth exists in your country, is your legal framework providing for a specific regulation? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	Health Records Act, No. 55/2009 and a Regulation on health records. Security of personal data in health information systems is subject to the Act on the Protection of Privacy as regards the Processing of Personal Data, no. 77/2000
Case-law:	None
Other:	Guidelines from the Directorate of Health on the security and quality of health records.

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
EHR and Medical data:	What can be considered medical data in your country? Is it solely the data relating to a person's health (state, diagnosis, prognosis, medical treatment, etc.)? Is non-medical data that leads to medical information treated the same way as medical data (for instance in terms of confidentiality requirements)? Is the EHR solely constituted of data collected in a medical context or can the individual also himself or herself add information regarding his or her health?
	Health data are defined as a description or interpretation in writing, images,

	including x-rays, graphical data and video and audio recordings, containing information regarding a patient's health and his/her treatment provided by a healthcare professional or healthcare facility, and other necessary personal data. Only healthcare practitioners and other staff, and students undergoing clinical/health training (internship) in healthcare sciences who have undertaken an obligation of confidentiality comparable to that of healthcare practitioners, may enter health data in health records In health records, all information necessary with respect to the patient's treatment shall be systematically entered.
Sharing of data and Access:	Who is granted access to the EHR and how is the sharing of information (with other health care providers?) regulated? Where information is shared with pharmacists, is there a strict purpose limitation in place? How has the definition of the responsibility over the medical data been regulated?
	The Health Records Act (no. 55/2009) states that healthcare professionals who are involved in a patient´s treatment shall have access to the patient´s health records. However, a patient can prohibit access to his/her health records. Under such circumstances the patient shall be informed that refusal to authorize necessary access to the health record may be equivalent to refusal of treatment. Furthermore, a patient or his/her representative has the right of access to his/her own health records. It is the supervisor of the health records at each health care facility that grants the access upon a written request. Moreover, healthcare authorities which by law receive for consideration a complaint from a patient or his/her representative with respect to treatment are entitled to access the patient's health records in the same manner as the patient himself/herself. Medication data are shared with pharmacists. Responsibility over medical data is regulated by the Health Records Act (no. 55/2009), Regulation no. 550 and the Medicinal Products Act no. 93/1994.
Data quality:	Are the principles of legitimacy, fairness and minimisation applied to medical data? How are records kept accurate? How long is the data kept for, is the specific storage period defined for the EHR?
	Yes, strict laws apply to medical data and the processing of medical data. The Health Records Act identifies minimum information to be systematically entered in the health record with respect to the patient´s treatment. Furthermore, the Directorate of Health issues guidelines, Minimum Data Sets, and mandated classification systems for use within health care. No, with respect to the obligation to pass health records to the National Archives for storage, the provisions of the National Archives Act apply.
Data integrity:	Are any specific methods used to ensure the integrity of the data? How are patients identified in the EHR? In the context of research, are anonymisation methods used and what safeguards exist for re-identification?
	Only authorized health professionals can enter or modify data within the EHR. It is prohibited by law to delete data, unless proven to be incorrect. Access is based on the individual and every step is traceable to that exact individual (the Act on Health Records no.55/2009). Every patient has a unique identifier (e.g. social security number).

	Yes, in the context of research strict procedures, law and regulations apply to safeguard personal health information (the Act on the Protection of Privacy as regards the Processing of Personal Data, no. 77/2000).
Data security:	Where are the records stored? Is there a centralised database of EHR? What security technology is being used?
	Most health institutions either store the EHR databases with a third party or themselves. The storage of health records needs to comply with the Act on Health Records no. 55/2009, the Health Records Regulation no. 550/2015 and the Directorate of Health directive on the quality and security of health records. Currently, there are two centralized databases; one for ePrescription and medication and another for immunization. Both are stored at the Directorate of Health.
Rights of the person/patient concerned:	How can the right of access be exercised? How can the data be corrected? Can the person enter information in his or her own EHR? What are the legal remedies available?
	A patient or his/her representative has the right of access to his/her own health records. It is the supervisor of the health records at each health care facility that grants the access upon a written request. Only the health professional who entered the data can make corrections, and the supervisor of health records. All changes are traceable, e.g. what was changed, when, and who changed it. No, patients cannot yet enter any information in their own EHR. Violations of the provisions of the Health Records Act entail fines, loose of licensure or even imprisonment for up to three years, depending on seriousness of the violation.
Consent:	Is the system based on an opt-in approach? Is the principle of granular consent applied (with the possibility of preventing access to certain data?)? If yes, in which situations?
	No, it is based on an opt-out approach. Yes, the patient can prohibit access to his/her health record.
Withdrawal:	Are patients able to withdraw the consent given to EHR schemes? If yes, what is the relevant procedure to withdraw such consent? What are the consequences?
	A patient can prohibit health care staff access to his/her EHR. The request has to be in written format, confirmed by a health practitioner and delivered to the supervisor of health records. Under such circumstances the patient shall be informed that refusal to authorize necessary access to the health record may be equivalent to refusal of treatment, as critical information may not be available to the health professional who has been denied access to the patient´s EHR. Moreover, a patient is entitled to information from the supervisor of health records regarding who has accessed his/her health record.
Outsourcing processing of data:	Is outsourcing common? Under what circumstances? Where is the data outsourced to? What sort of safeguards are in place?
	No, outsourcing is not common.

2. Cloud Computing, Data Mining and Profiling from both Medical Records (including EHR) and Data not specifically related to medical records.

2.1. Data Protection Issues:

Cloud computing has brought a new dimension to the way data is stored, accessed and processed. Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS), Network as a service (NaaS) are all used by services and organisations that deal with both medical data and non-medical data.

With the development of more advanced and efficient data-mining and data-querying Medical techniques (e.g NoSQL, MapReduce, Hadoop) in conjunction with increased processing power and data storage, mining data has never been more informative, easier, and cost-effective.

Healthcare is a natural sector in which to apply new technologies and methodologies, with particular impacts in epidemiology, public health, health services research, etc.

Data that can lead to the identification of a particular individual and his/her health situation is not limited to medical data *per se,* present on Electronic Health Records, but also to unsuspicious type of information.

There is a growing concern that these schemes may be implemented in manner which does not always respect the patients' confidentiality and basic rights, and in a broader context, the use of this of information may prejudice the individuals concerned.

The ability to track and monitor patients and resources enables a more efficient provision of care but may have an impact on the right to privacy of the individual concerned.

2.2. Questions: Is your legal framework providing for a regulation of Cloud Computing, Data Mining and Profiling? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	Act on the Protection of Privacy as regards the Processing of Personal Data, no. 77/2000 (implementation of Directive 95/46/EC)
Case-law:	None
Other:	The legal framework does not provide a specific regulation of Cloud Computing, Data Mining and Profiling. General data protection rules and special conditions regarding the processing of sensitive data apply. Rules regarding transfer of personal data have to be considered as well as provisions on risk assessment, security and integrity of personal data. Due to a heavy workload at the DPA, as well as financial restrictions, it has not been able to issue guidelines or opinions regarding the use of cloud computing, data mining and profiling in the health sector.

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Cloud computing:	How is cloud computing regulated in your country? Which security safeguards and standards are mandatory? Are there specific requirements in order to store medical data in the cloud? How is data shared and is the sharing regulated?
	Cloud computing is not regulated specifically, but the provisions of Act no. 77/2000 fully apply to all processing of personal data, including cloud computing, as well as the Act on Health Records no 55/2009.
Government:	Do governmental programmes exist to allow for increased data-mining of medical records? If yes, what are the purposes of this data mining? Are private entities allowed to access the data? Under what circumstances? What sort of techniques and technologies are being used? To what end? Are data subjects informed of this type of data-mining?

	The DPA has not had any cases regarding this issue, but general data protection rules would apply, i.e. where the data subject has given an informed consent.
Private sector:	Are private entities allowed to mine medical data which they process? Under what circumstances? Can the government have access to this data?
	The DPA has not had any cases regarding this issue, but general data protection rules would apply, i.e. where the data subject has given an informed consent.
Profiling:	Are the government and the private sector allowed to employ profiling methods on medical data? If yes, under what circumstances? Is it allowed to cross and correlate non-medical data with medical data?
	Provisions of Act No. 77/2000 apply, no specific provisions on profiling methods on medical data exist. The DPA has not had any cases regarding this issue, but general data protection rules would apply, i.e. where the data subject has given an informed consent.

3. RFID and wireless communication technologies

3.1. Data Protection Issues:

It is common for medical devices, such as patients' tags, to possess RFID technologies in order to facilitate the transmission of the patients' data.

It can also be related to the data-mining operations previously mentioned as it is another category of information that can be used to discern meaningful patterns.

Transmission of data through radio-frequency is not limited to medical devices. Almost any smartphone uses some technology enabling to collect, and share, the user's data. For instance, via WI-FI it is possible to identify users' locations and therefore infer some of their behaviour, which in some cases can relate to health information.

3.2. Questions: Is your legal framework providing for a regulation of RFID technologies and the transfer of personal data through wireless technologies? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	No specific regulation on RFID technologies exist. Act No. 77/2000 applies as regards to the processing of personal data.
Case-law:	No case law exists
Other:	No guidelines or opinions from the DPA exist.

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
RFID:	How is RFID used in hospital/clinics for (a) resource management, (b) patient care? What types of database systems (and security) are implemented in conjunction with RFID use? How are issues of access, sharing, consent etc. managed considering that RFID may be used without the patients' knowledge.
	RFID has not been used in hospitals/clinics in Iceland, neither for resource management nor for patient care.
Wireless tracking technologies:	Are hospitals/clinics employing other wireless tracking technologies besides RFID? Which ones? Do they have to follow specific security requirements? Which ones?
	No, they are not.

4. Applications (Mobile)

4.1. Data Protection Issues:

Information society is increasingly relying on the use of “apps” (application), most of them mobile. These apps are commonly designed to gather personal data, and in practice often process medical data.
Technologies such as multi-touch touchscreen, accelerometers or gyroscopes, ambient light sensors, GPS and cameras, and devices featuring fingerprint and biometric sensors also involve the collection of medical data.

A mobile phone application can monitor accurately physiological data, such as heartbeats, sleep patterns, fitness information.

4.2. Questions: Is your legal framework providing for a regulation of Apps and Mobile Apps? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs’ opinions and/or case law.	
Legislation:	No specific legal framework regulates Apps or Mobile apps as regards to medical data. Act No 77/2000 applies to all processing of personal data.
Case-law:	No specific case-law exists.
Other:	No opinions or guidelines of the DPA exists

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs’ opinions and/or case law).	
Apps:	Is it allowed to use apps and mobile apps to deploy medical services and collect medical data? If yes, which type of individual/organisation can develop and employ these apps? Are there specific security requirements for these types of apps?
	If personal data is being processed with apps or mobile apps it has to fulfill the requirements of Act No 77/2000, i.e. general rules regarding the processing of personal data (Art. 8) and specific conditions regarding the processing of sensitive data (Art. 9). Also the controller has to make sure that his ISMS is in accordance with the provisions of the Act regarding risk assessment, security and integrity of personal data (Art. 11).
Institutions:	Do hospitals/clinics/labs employ apps to gather medical data? Is there a need for a medical treatment to permit the use of an app to process the medical data? Are there specific security requirements for the institutions collecting these data from the apps? Are medico-administrative data used by hospitals/clinics for management purposes?
	No, hospitals/clinics/labs are not using apps to gather medical data in Iceland.
Tracking technologies:	Do hospitals/clinics/labs employ non-medical apps and devices to track and collect data from their patients? What type of data is collected? For what purpose? Is the data identifiable? Is the data combined with medical data?
	No, hospitals/clinics/labs do not employ non-medical apps and devices to track or collect data from their patients.
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical apps and tracking apps? If yes, what are the standards?
	No specific requirements are made in the Act No. 77/2000, apart from provisions regarding risk and safety measures (Art. 11). The DPA has also set specific rules on the security of personal data.

Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical diagnostic? How would this be applied to fitness and daily-basis data?

5. Medical Devices and Wearable Devices

5.1. Data Protection Issues:

A medical device can be defined as: 'any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application. Such a device should be intended by the manufacturer for one of a number of defined purposes, one of which is, diagnosis, prevention, monitoring, treatment or alleviation of disease' (Directive 93/42/EEC Article 1:2)

Some eHealth and mHealth devices and apps do not fall in this definition of medical devices, as can also be the case of a software working in combination with a physical device, for instance a smartphone.

5.2. Questions: Is your legal framework providing for a regulation of Medical Devices? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	If such devices process personal data Act No. 77/2000 applies. Act no. 16/2001 on Medical Devices applies for Medical Devices in Iceland. Act no. 16/2001 on Medical Devices does not address personal data protection directly only production and marketing of medical devices and their safety. Act 16/2001 on medical Devices is the basis for Icelandic regulations implementing EU Medical Directives. All Medical Devices shall be CE marked
Case-law:	No case law exists.
Other:	No guidelines or opinions have been issued by the DPA.

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
eHealth and mHealth:	Does the concept of Medical device in your country encompass services and apparels in the realm of eHealth and mHealth? What are the requirements? Should, for instance, the medical device be certified before it can be used?
	Software which falls under the definition of Medical Devices in the MD Directives is regulated by Act 16/2001 on Medical Devices. All Medical Devices shall be CE marked.
Apps:	Does the concept of medical devices encompass apps? If yes, is there any regulation applicable to apps that perform medical services? Is there any regulation applicable on apps that track non-medical data that can lead to health information? If yes, what type of data?
	Software which falls under the definition of Medical Devices in the MD Directives is regulated by Act 16/2001 on Medical Devices. All Medical Devices shall be CE marked.

Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical and/or wearable devices? If yes, what are the standards?
	No specific requirements are made in the Act No. 77/2000, apart from provisions regarding risk and safety measures (Art. 11). The DPA has also set specific rules on the security of personal data. Act No. 16/2001 on Medical Devices does not address privacy directly.
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical treatment? How would this be applied to fitness and daily-basis data?
	No. Software which falls under the definition of Medical Devices in the MD Directives are regulated by Act 16/2001 on Medical Devices

6. Internet of Things

6.1. Data Protection Issues:

Internet of things relates to common, ordinary devices that are now, and increasingly, connected to the Internet, such as cars, fridges, ovens, microwaves, etc. All of these devices can provide data that can lead to reveal information concerning one's health. A fridge can easily inform on the type of food stored and thus the diet of an individual. One of the biggest challenges of the Internet of Things is to guarantee the right to privacy and data protection in a world where every device collects, processes, analyses and transmits the data, commonly via wireless technologies.

In the realm of medical data, the issue mainly arises when crossing seemly unrelated data that can lead to health information about an individual.

6.2. Questions: Is your legal framework providing for a regulation of the Internet of Things? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	If such devices process personal data the provisions of Act No. 77/2000 apply.
Case-law:	No case-law exists
Other:	No guidelines or opinions have been issued by the DPA.

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Security:	What are the security standards that need to be employed by these devices when collecting personal data?
	Art. 11 of Act 77/2000 as well as provisions of rules no. 299/2001, on security of personal data.
Non-medical devices:	Are non-medical devices allowed to collect medical data, such as heart frequency? Are they allowed to cross medical data with non-medical data?
	The DPA has not had any cases regarding this issue, but general data protection rules would apply, i.e. where the data subject has given an informed consent.
Privacy by Design:	Is there any requirement to implement privacy by design in the development of connected devices? If yes, what are the standards?

	No.

7. Electronic Doctor (online Doctor) and on-line appointments

7.1. Data Protection Issues:

The Doctor listens, talks and assesses the patient online, via a website, app, canal, sometimes including video-conference. Medical data is collected and processed, what are the security requirements and standards followed? Other websites provide for on-line appointments with doctors, which can also involve the processing of medical data.

7.2. Questions: Is your legal framework providing for a regulation of online Medical Treatment and is the on-line appointment system covered by such a framework? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	If the controller uses such framework when processing personal data the provisions of Act No. 77/2000 apply.
Case-law:	No specific case law.
Other:	No opinions or guidelines have been issued.

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Medical treatment:	Is it allowed to perform medical treatment via online services? If yes, how should the medical services be provided? Does it have to follow the same requirements of a regular physically-present medical treatment?
	Online medical services shall only be performed via a secure health net. Provisions of the Act on Health Services no. 40/2007 and the Health Records Act no.55/2009 apply.
Medical data:	How should the data collected via a medical treatment performed online be processed? Are there specific requirements? Which ones?
	Provisions of the Act on Health Services no. 40/2007 and the Health Records Act no.55/2009 apply, as well as the Act on the Protection of Privacy as regards the Processing of Personal Data, no. 77/2000.

Other comments and technologies
Should you wish to describe any technology, feature or trend that has not been covered by the questionnaire, please feel free to use the space provided below. Where relevant, also indicate recent legislation changes, guidelines and/or case law.

ITALY / ITALIE

QUESTIONNAIRE

The questionnaire should ideally be completed by data protection authorities, health policy authorities, professional or patient associations as well as healthcare providers: you are invited to share it as widely as possible.

Please send your replies to dataprotection@coe.int no later than 15 December 2014.

1. Mobile Health (mHealth) and Electronic Health Records (EHR)

1.1. Data Protection Issues:

This is perhaps the biggest topic sitting at the intersection of technology and data protection. Mobile health (mHealth) and Electronic Health Records (EHR) are increasingly used in healthcare systems and provisions – it is a trend that needs to be examined.

Related to the EHR, these records are more accurate, cost-effective (in terms of storage) than paper-based notes. The concept of patient controlled/accessed EHR has been implemented in varying degrees in different countries.

Furthermore, some non-medical record can still contain health information about users and it should be considered if such records ought to be treated in a similar way to EHR.

Also, should 'medical data' as defined in Recommendation N° (97) 5 on the protection of medical data cover physical tracking data, such as pedometers or fitness data and data that can lead to medical information about an individual ?

1.2. Questions: if EHR exist in your country, is your legal framework providing for a regulation of such records? If mHealth exists in your country, is your legal framework providing for a specific regulation? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	With regard to EHR, the legal framework is Section 12 of Decree Law no. 179/2012 which, amongst others, sets forth the purposes of EHR, the bodies in charge of pursuing the different scopes, and the access requirements (based on data subject's consent). Please note that Section 12.2 explicitly refers to the data protection requirements provided for by the Italian Data Protection Code (legislative decree 196/2003, available, in English, at the following link: http://194.242.234.211/documents/10160/2012405/DataProtectionCode-2003.pdf) According to Section 12.7, the Ministry of Health must issue one or more decrees for the full implementation of section 12 of decree 179/2012. The adoption of the first implementation decree is forthcoming. According to Art. 12 of Decree Law no. 179/2012 the Electronic Health Record is defined "as a set of digital data and documents relating to health and social health clinical events generated by present and past, regarding the patient, which is intended to facilitate patient care, provide a service that can foster the integration of different skills, deliver a consistent information base, contributing to the improvement of all activities and nursing care, in compliance with the regulations for the protection of personal data". Activities have been planned for the implementation of Electronic Health Record systems at regional level. Decree Law no. 69/2013 established that consent or refusal for organ donation falls within

	the EHR (Article 43, paragraph 1a). Please note that our legal framework does not provide for a specific regulation of mHealth. However, the Data Protection Code applies in this sector too, including some specific provisions concerning data processing within electronic communication sectors (See Title X of the DPCode).
Case-law:	-
Other:	**EHR:** In respect of EHR, Guidelines on the Electronic Health Record and the Health File were adopted by the Italian Data Protection on 16 July 2009 (available in English at: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1672821) The Guidelines, which drew inspiration from the work of the Article 29 Working Party (see the Working Document adopted on 15 February 2007 http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp131_en.pdf), were issued by the DPA - pending at that time the enactment of specific legislation - following a public consultation that involved the relevant practitioners; They lay down a first set of rules to ensure the protection of medical data and safeguard individuals. Moreover, on 22 May 2014 the Italian DPA adopted an opinion on the first draft Decree implementing Decree 179/2012, which sets forth the information and documents to be included in the EHR, the responsibilities and tasks of the different entities/subjects involved, the data protection safeguards and security measures to be adopted, the criteria for accessing the EHR, and the interoperability criteria. The (favourable) Opinion is available (only in Italian) at: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3230826) **mHealth:** The Italian DPA participated in the second annual Global Privacy Enforcement Network (GPEN) Privacy Sweep, concerning apps. https://www.priv.gc.ca/media/nr-c/2014/nr-c_140910_e.asp Our DPA decided to focus on health apps. The results of the Italian sweeping activity showed that the degree of transparency on the processing of users' data and the permissions required to download the selected medical Apps, in some cases, are not in line with the Italian data protection legislation. 50% of App showed lack of "privacy pre-installation communications" (i.e. privacy policy prior to the App installation) or too general privacy policies or not tailored for the smart phone/tablet small screen, or even hidden in the credit section. As for Italian DPA's tasks, at the national level, the Authority is planning an assessment in terms of needed inspections and any possible prescriptive measures/sanctions. (See press release: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3375236)

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
EHR and Medical data:	What can be considered medical data in your country? Is it solely the data relating to a person's health (state, diagnosis, prognosis, medical treatment, etc.)? Is non-medical data that leads to medical information treated the same way as medical data (for instance in terms of confidentiality requirements)? Is the EHR solely constituted of data collected in a medical context or can the individual also himself or herself add information regarding his or her health?
	Definition of health data: According to Section 4, paragraph 1, letter d) of the DPCode, **personal data disclosing health** are "sensitive data" and therefore subject to specific safeguards (as provided for by Article 6 of Convention 108/1981 and Article 8 of Directive 95/46). Although there is not a definition of medical data in the DPCode, the concept of "personal

	data disclosing health" – which enjoy even stricter safeguards among sensitive data - is broad enough to cover all those data enabling the disclosure of health. For example, on several occasions the Italian DPA considered the information concerning the illness status in an employment sector (in case of absence for illness) to be health data. See in particular "Guiding Principles Applying to the Processing of Employees' Personal Data for the Purpose of Managing Employment Relations in the Private Sector" http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1427027, see Sections 5.3 and 6.1) and Guiding principles on the processing of employees' personal data in the public sector http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1693793 - See Section 6.3). Also the reference, associated to an individual, to a law providing for benefits for certain categories of people (such as people with disabilities) may fall under the notion of health data and be therefore subject to special protection. Please note that the European Data Protection Supervisor (EDPS) has focused on the concept of health data on several occasions. See for example: - "Guidelines concerning the processing of health data in the workplace by Community institutions and bodies" ("Health data generally refers to personal data that have link with the health status of a person. This would normally include medical data (e.g. doctor referrals and prescriptions, medical examination reports, laboratory tests, radiographs), as well as administrative and financial data relating to health (e.g. medical appointments scheduling, invoices *for healthcare service provision, indication of the number of days of sick leave, sick leave management"*). https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Supervision/Guidelines/09-09-28_Guidelines_Healthdata_atwork_EN.pdf - Opinion on the Communication from the Commission on 'eHealth Action Plan 2012-2020 - Innovative healthcare for the 21st century https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2013/13-03-27_eHealth_Action_EN.pdf - Opinion on the proposal for a directive of the European Parliament and of the Council on the application of patients' rights in cross-border healthcare https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2008/08-12-02_Crossborder_healthcare_EN.pdf **Additional data on EHR:** According to Section 5 of the said forthcoming first implementation decree (in application of the section 12 (7) of D.L. 179/2012), the individual can add information by herself/himself on a specific section of the EHR called "personal notebook".
Sharing of data and Access:	Who is granted access to the EHR and how is the sharing of information (with other health care providers?) regulated? Where information is shared with pharmacists, is there a strict purpose limitation in place? How has the definition of the responsibility over the medical data been regulated?
	According to Sections 10, 14, 18 and 21 of the said forthcoming first implementation decree of the Ministry of health, the following subjects are allowed to access the EHR: patient (data subject), Regions and Autonomous Provinces, Health Regional Services and Social-health Regional Services, Ministry of Health. According to Section 12 (2 bis) of D.L. 179/2012, the pharmacist will be allowed to access with the only purpose to view the medical prescriptions. The responsibility over the medical data is regulated according to Sections 28-30 of the DPCode. In respect of the role and responsibilities allocated on data controllers and processors, see also the abovementioned Guidelines on EHR issued by the Italian DPA

	http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1672821, in particular Section 2 and 4.
Data quality:	Are the principles of legitimacy, fairness and minimisation applied to medical data? How are records kept accurate? How long is the data kept for, is the specific storage period defined for the EHR?
	Legitimacy, fairness and minimisation are general data protection principles (Sections 3 and 11) that *a fortiori* apply to medical data. The data are updated each new healthcare performance, unless the data subject decides to obscure the information for any reason. The specific storage period for the EHR is not defined. Please note that in the said Guidelines (see previous answer) the DPA stated that if consent is withdrawn the EHR the medical records contained therein should be further available to the health care bodies that have drafted them (this applies, for instance, to the hospitalization information that may be used by the given hospital), without prejudice moreover to their retention where required under the law; however, they should no longer be shared among the other health care bodies/professionals treating the given data subject (Section 22(5) of the DP Code).
Data integrity:	Are any specific methods used to ensure the integrity of the data? How are patients identified in the EHR? In the context of research, are anonymisation methods used and what safeguards exist for re-identification?
	Data integrity (and security) The ongoing implementing decree provides for appropriate measures aiming at security and integrity of data such as: - authentication and authorisation systems applied to the persons in charge for the processing as a function of the respective access/processing requirement; - procedures to regularly check quality and consistency of authentication credentials and authorisation profiles applying to the persons in charge for the processing; - criteria to encrypt and/or keep separate the data suitable for disclosing health and sex life from any other personal data; - logging of accesses and operations; - audit logging to control database accesses and detect abnormalities; - secure communication protocols by implementing encryption standards for electronic data communications between the various data controllers. Such measures were contained in the said Guidelines on EHR adopted by the DPA in 2009. The said decree also provides for the obligation for the data controller to notify data breaches to the DPA. Such measure was also suggested by the DPA in its Opinion of 22 May 2014 on the draft decree http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3230826). **Identification of the patient:** In the EHR, the patient is identified with name, last name and tax code. The data required for the correct identification of the patient in feeding the EHR are listed in a Technical Annex of the decree. **Research** In the context of research pseudo-anonymisation methods are adopted. The specific safeguards provided for by the Code of conduct on processing of personal data for scientific and statistical purposes, attached to the DPCode, must be also ensured.
Data security:	Where are the records stored? Is there a centralised database of EHR? What security technology is being used?
	The records are stored from data controllers in their archives. There is not a centralized database of EHR. In respect of security, please see the previous answer.
Rights of the person/patient	How can the right of access be exercised? How can the data be corrected? Can the person enter information in his or her own EHR? What are the legal remedies available?
	Rights of access and correction can be both exercised according to the Section 7 of the DPCode.

concerned:	As mentioned before, the data subject is allowed to add data related to her/him on a specific section of the EHR. With regard to remedies, the rights as per Section 7 may be enforced either by filing a lawsuit or by lodging a complaint with the Garante. The DPA is not competent for compensation of damages (See Section 15 of the DPCode) which is left to the judicial competence. Remedies before the DPA are set forth by Section 141-151 (claims to point out an infringement of the relevant provisions on the processing of personal data; report to call upon the DPA to check up on the data protection provisions; complaints with a view to establishing the specific rights referred to in Section 7).
Consent:	Is the system based on an opt-in approach? Is the principle of granular consent applied (with the possibility of preventing access to certain data?)? If yes, in which situations?
	The system is based on an opt-in approach. The refusal to have an EHR should not affect the patient's right to medical care. The principle of the granular consent is applied. The patient can choose which information should be stored, from whom information can be viewed and whether to blank some information. A mechanism of “blank the blanking” is also provided, as also suggested by the DPA in the said Guidelines on EHR.
Withdrawal:	Are patients able to withdraw the consent given to EHR schemes? If yes, what is the relevant procedure to withdraw such consent? What are the consequences?
	The patients are always able to withdraw the given consent, according to the Section 8(6), of the forthcoming first implementation decree of the Ministry of health (in application of the section 12 (7) of D.L. 179/2012). There are no consequences for, as mentioned before, patient's right to medical care is guaranteed even in case of refusal or withdrawal to have an EHR.
Outsourcing processing of data:	Is outsourcing common? Under what circumstances? Where is the data outsourced to? What sort of safeguards are in place?
	None of the contributions to the questionnaire received refers to cases of outsourcing. In respect of its institutional activity related to EHR, the Italian DPA has not experienced any case of outsourcing so far.

2. Cloud Computing, Data Mining and Profiling from both Medical Records (including EHR) and Data not specifically related to medical records.

2.1. Data Protection Issues:

Cloud computing has brought a new dimension to the way data is stored, accessed and processed. Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS), Network as a service (NaaS) are all used by services and organisations that deal with both medical data and non-medical data.

With the development of more advanced and efficient data-mining and data-querying Medical techniques (e.g NoSQL, MapReduce, Hadoop) in conjunction with increased processing power and data storage, mining data has never been more informative, easier, and cost-effective.

Healthcare is a natural sector in which to apply new technologies and methodologies, with particular impacts in epidemiology, public health, health services research, etc.

Data that can lead to the identification of a particular individual and his/her health situation is not limited to medical data *per se,* present on Electronic Health Records, but also to unsuspicious type of information.

There is a growing concern that these schemes may be implemented in manner which does not always respect the patients’ confidentiality and basic rights, and in a broader context, the use of this of information may prejudice the individuals concerned.

The ability to track and monitor patients and resources enables a more efficient provision of care but may have an impact on the right to privacy of the individual concerned.

2.2. Questions: Is your legal framework providing for a regulation of Cloud Computing, Data Mining and Profiling? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	**Cloud computing**: There is not a specific legal specific framework for cloud computing. However, data protection principles, as provided for by the DPCode, should apply as in any other sector. **Profiling**: A specific provision of the DPCode concerns "Profiling of Data Subjects and Their Personality" (Section 14). According to such provision, no judicial or administrative act or measure involving the assessment of a person's conduct may be based solely on the automated processing of personal data aimed at defining the data subject's profile or personality. Moreover, the data subject may challenge any other decision that is based on such kind of processing.
Case-law:	-
Other:	As regards cloud computing, the Italian DPA decided to issue a "mini-vademecum" called "Cloud Computing – Protect Your Data without Falling from a Cloud". The vademecum, which concerns cloud computing in general and not only the health sector, includes specific examples and a Decalogue with practical tips and suggestions for further analysis. http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1906181 Data mining and Profiling were considered by the DPA on several occasions (prior checking under Section 14 and 17 of the Code) although more in connection with the tlc sector, electronic communications and marketing. Please note that with a Decision of 7 December 2006 the DPA dealt with a case where personal data related to pregnant women, in neonatal health facilities or clinics, were collected - for marketing purposes - by a publisher of a review on childhood, with the help of the personnel of the clinic who received gifts and benefits from the publisher. With that decision, the DPA prohibited the processing which had been carried out in violation of several DPCode provisions, including transparency obligations, designation of controller/processor, and exercise of data subject's rights. See http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1379101

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Cloud computing:	How is cloud computing regulated in your country? Which security safeguards and standards are mandatory? Are there specific requirements in order to store medical data in the cloud? How is data shared and is the sharing regulated?
	See previous answers.
Government:	Do governmental programmes exist to allow for increased data-mining of medical records? If yes, what are the purposes of this data mining? Are private entities allowed to access the data? Under what circumstances? What sort of techniques and technologies are being used? To what end? Are data subjects informed of this type of data-mining?
	In the Ministry of Health, the New Health Information System (NSIS) is the information system dedicated to governance purposes. Data-mining initiatives are still in an early phase of scope definition. The law provides for the possibility to interconnect health records at national level but only by using unique codes related to patients.

Private sector:	Are private entities allowed to mine medical data which they process? Under what circumstances? Can the government have access to this data?
	Private entities can mine medical data obtaining the consent from data subject or using irreversibly anonymized data. The government can access to this data, in aggregated form, and only for health quality assessment purposes.
Profiling:	Are the government and the private sector allowed to employ profiling methods on medical data? If yes, under what circumstances? Is it allowed to cross and correlate non-medical data with medical data?
	For any cross connection, correlation or profiling activity, the general legal framework applies. The scope of treatments in the public sector does not include profiling for governance purposes. A specific regulation for a comprehensive cross-connection among different medical information in NSIS is ongoing.

3. RFID and wireless communication technologies

3.1. Data Protection Issues:

It is common for medical devices, such as patients' tags, to possess RFID technologies in order to facilitate the transmission of the patients' data.

It can also be related to the data-mining operations previously mentioned as it is another category of information that can be used to discern meaningful patterns.

Transmission of data through radio-frequency is not limited to medical devices. Almost any smartphone uses some technology enabling to collect, and share, the user's data. For instance, via WI-FI it is possible to identify users' locations and therefore infer some of their behaviour, which in some cases can relate to health information.

3.2. Questions: Is your legal framework providing for a regulation of RFID technologies and the transfer of personal data through wireless technologies? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	Italy does not have a specific legal framework for RFID technologies and the transfer of personal data through wireless technologies. Data protection requirements, as provided for by the DPCode, apply in this sector too.
Case-law:	-
Other:	On 9 March 2005, the DPA adopted a general decision setting forth the specific safeguards to be put in place while processing data through the use of RFID: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1109493 Moreover, with a decision adopted 29 November 2012 following a prior checking request (Section 17 of the DPCode), the DPA dealt with the processing of personal data through RFID for the remote monitoring of patients with implantable cardiac defibrillators. The DPA prescribed to both the hospital and the producer of the RFID device adequate measures to be adopted in order to ensure the full compliance with the DPCode. (data subject's consent, possibility for an easy deactivation of the remote control device, stringent data security measures, specific safeguards for the outsourcing of certain activities regarding security checks on the said devices). http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2276103

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
RFID:	How is RFID used in hospital/clinics for (a) resource management, (b) patient care? What types of database systems (and security) are implemented in conjunction with

	RFID use? How are issues of access, sharing, consent etc. managed considering that RFID may be used without the patients' knowledge.
	No information was provided regarding this issue.
Wireless tracking technologies:	Are hospitals/clinics employing other wireless tracking technologies besides RFID? Which ones? Do they have to follow specific security requirements? Which ones?
	No information was provided regarding this issue. In respect of security requirements see the abovementioned decisions by the DPA, respectively of 9 March 2005 and 29 November 2012.

4. Applications (Mobile)

4.1. Data Protection Issues:

Information society is increasingly relying on the use of "apps" (application), most of them mobile. These apps are commonly designed to gather personal data, and in practice often process medical data.
Technologies such as multi-touch touchscreen, accelerometers or gyroscopes, ambient light sensors, GPS and cameras, and devices featuring fingerprint and biometric sensors also involve the collection of medical data.

A mobile phone application can monitor accurately physiological data, such as heartbeats, sleep patterns, fitness information.

4.2. Questions: Is your legal framework providing for a regulation of Apps and Mobile Apps? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	There is not a specific regulation concerning Apps and Mobile Apps. Nevertheless, the processing of data in this field should be carried out in the due respect for data protection principles as set forth by the DPCode.
Case-law:	-
Other:	As stated before, the Italian DPA, following the Sweep initiative, announced inspections and possible prescriptive measures/sanctions concerning the processing of data related to medical apps. The DPA actively took part in the elaboration of the Article 29 Working Party's Opinion 2/2013 on apps on smart devices http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Apps:	Is it allowed to use apps and mobile apps to deploy medical services and collect medical data? If yes, which type of individual/organisation can develop and employ these apps? Are there specific security requirements for these types of apps?
	Yes, it is allowed to use apps and mobile apps to deploy medical services and collect medical data but the data controller must comply with the current legal framework, including data protection requirements. In order to answer to this and the following questions regarding security requirements, it is important to consider that there are several subjects intervening in the processing of data related to the use of apps ("app developers", including "app owners", "app stores", etc.) who are called upon to ensure fulfillment of DP requirements. The roles and responsibilities of the different subjects involved, in particular concerning security measures has been analysed by the Article 29 Working Party in the said Opinion 3/2013 to which we refer to (See in particular section 3.3. and 3.7 of the Opinion)
Institutions:	Do hospitals/clinics/labs employ apps to gather medical data? Is there a need for a

	medical treatment to permit the use of an app to process the medical data? Are there specific security requirements for the institutions collecting these data from the apps? Are medico-administrative data used by hospitals/clinics for management purposes?
	No specific answers were provided on the employment of apps in hospital/clinics/labs. Hospital/clinic/labs must respect the security requirements provided for by Sections 31-36 of the DPCode, including the specific safeguards in case of processing of data disclosing health performed by health care bodies by electronic means (encryption techniques or identification codes. see Section 34, para 1, lett. h). Please note that technical specifications concerning minimum security measures are contained in the Annex B of the DPCode, including in respect of the processing carried out by health care bodies and professionals on data disclosing health and sex life. Medical-administrative data could be used by hospitals/clinicsfor management purposes always in the due respect of data protection principles.
Tracking technologies:	Do hospitals/clinics/labs employ non-medical apps and devices to track and collect data from their patients? What type of data is collected? For what purpose? Is the data identifiable? Is the data combined with medical data?
	No information has been provided on this issue
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical apps and tracking apps? If yes, what are the standards?
	Although there is not a specific privacy by design requirement for medical and tracking apps, Section 3 of the DPCode, which applies to data processing in any sector, states that information systems and software must be configured by minimising the use of personal data and identification data, in such a way as to rule out their processing if the purposes sought in the individual cases can be achieved by using either anonymous data or suitable arrangements to allow identifying data subjects only in cases of necessity, respectively.
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical diagnostic? How would this be applied to fitness and daily-basis data?
	The system should be based on opt-in. The collection of data should be justified by medical purposes (such as prevention, diagnosis, treatment, etc.). Generally speaking, the DPCode requires the data subject's (written) consent for any processing of health data (online "clicking" is considered to be equivalent to a written consent). Such rule would be applied also to fitness and daily-basis data as long as such data disclose information on the individual's health.

5. Medical Devices and Wearable Devices

5.1. Data Protection Issues:

A medical device can be defined as: 'any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application. Such a device should be intended by the manufacturer for one of a number of defined purposes, one of which is, diagnosis, prevention, monitoring, treatment or alleviation of disease' (Directive 93/42/EEC Article 1:2)

Some eHealth and mHealth devices and apps do not fall in this definition of medical devices, as can also be the case of a software working in combination with a physical device, for instance a smartphone.

5.2. Questions: Is your legal framework providing for a regulation of Medical Devices? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	Yes, the Italian legal framework provides for the regulation of medical device or in-vitro device according the Directive 93/42/EEC concerning medical devices (Legislative Decree 24 February 1997 no 46 http://www.salute.gov.it/imgs/C_17_normativa_515_allegato.pdf) and Directive 98/79/EC on in vitro diagnostic medical devices (Legislative Decree September 2000, no. 332 http://www.salute.gov.it/imgs/C_17_normativa_544_allegato.pdf)
Case-law:	-
Other:	-

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
General answer: On 26 September 2012, the European Commission adopted two Proposals, one for a Regulation on medical devices and the other for a Regulation on in vitro diagnostic medical devices which, once adopted, will replace the existing legal framework applicable to medical devices in EU. There are no binding rules in EU as to the difference between lifestyle and wellbeing apps and a medical device or in vitro diagnostic medical device. Since January 2012, in order to help software developers and manufacturers identify whether their products fall or not under the Directive on medical devices or the Directive on in vitro diagnostic medical devices, the Commission's services issued some guidance which will be continuously updated (Guidelines on the qualification and classification of stand-alone software used in healthcare within the regulatory framework of medical devices, MEDDEV 2.1/6 January 2012). These Guidelines are, at the moment, the only legal framework for app and software used in healthcare.	
eHealth and mHealth:	Does the concept of Medical device in your country encompass services and apparels in the realm of eHealth and mHealth? What are the requirements? Should, for instance, the medical device be certified before it can be used?
	See the previous answer
Apps:	Does the concept of medical devices encompass apps? If yes, is there any regulation applicable to apps that perform medical services? Is there any regulation applicable on apps that track non-medical data that can lead to health information? If yes, what type of data?
	See the previous answer
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical and/or wearable devices? If yes, what are the standards?
	See, as per answer 4.2,Section 3 of the DPCode.
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical treatment? How would this be applied to fitness and daily-basis data?
	See answer 4.2

6. Internet of Things

6.1. Data Protection Issues:

Internet of things relates to common, ordinary devices that are now, and increasingly, connected to the Internet, such as cars, fridges, ovens, microwaves, etc. All of these devices can provide data that can lead to reveal information concerning one's health. A fridge can easily inform on the type of food stored and thus the diet of an individual. One of the biggest challenges of the Internet of Things is to guarantee the right to privacy and data protection in a world where every device collects, processes, analyses and transmits the data, commonly via wireless technologies.

In the realm of medical data, the issue mainly arises when crossing seemly unrelated data that can lead to

health information about an individual.

6.2. Questions: Is your legal framework providing for a regulation of the Internet of Things? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	There is not a specific legal framework providing for internet of things. As in any other sector the DPCode should apply.
Case-law:	-
Other:	-

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Security:	What are the security standards that need to be employed by these devices when collecting personal data?
	In respect of data security, the requirements provided for by the DPCode should apply.
Non-medical devices:	Are non-medical devices allowed to collect medical data, such as heart frequency? Are they allowed to cross medical data with non-medical data?
	No information has been provided on this issue.
Privacy by Design:	Is there any requirement to implement privacy by design in the development of connected devices? If yes, what are the standards?
	Again see Section 3 of the DPCode, which applies to any sector.

7. Electronic Doctor (online Doctor) and on-line appointments

7.1. Data Protection Issues: The Doctor listens, talks and assesses the patient online, via a website, app, canal, sometimes including video-conference. Medical data is collected and processed, what are the security requirements and standards followed? Other websites provide for on-line appointments with doctors, which can also involve the processing of medical data.

7.2. Questions: Is your legal framework providing for a regulation of online Medical Treatment and is the on-line appointment system covered by such a framework? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	The Ministry of the Health set up within the National Health Council (CSS), a working group for Telemedicine. The working group is composed of members and experts of the CSS, General Managers and representatives of the Ministry of Health. This working group defined specific national guidelines ("Telemedicina, linee di indirizzo nazionali") which have been adopted with a State-Regions agreement on February 20, 2014. http://www.salute.gov.it/imgs/C_17_pubblicazioni_2129_allegato.pdf There are also few regional laws on telemedicine. Again, the general data protection legislation is the DPCode.
Case-law:	-
Other:	Please note that on 25 January 2012 the DPA issued "Guidelines on processing personal data for dissemination and publication on exclusively health-related web sites". Such guidelines refer to the processing of personally identifying and/or sensitive data relating to users on exclusively health-related web sites – where one can ask for advice, exchange information, and share comments. The guidelines point out the safeguards to be adopted so that such processing is performed in compliance with personal data protection legislation, in particular, by ensuring that the data in question are relevant and not excessive and that they are processed fairly and in good faith (see section 11 of the

	Code): http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1879894 The Italian National Bioethics Committee (CNB) issued an Opinion on Ethics, Health and New Information Technologies (21st of April 2006), whereby recommending that "in the training of a doctor, specialist and healthcare personnel, it will be important to insist also on ethico-legal problems concerning the protection of "privacy" and caution in the preservation, processing and transmission via the internet etc. of the patient's health data, according to international and national binding regulations. The doctor and in general the health operator, when required and interested in professional communication on the internet, must, deontologically, keep sight of the "human" complexity of the doctor/patient relationship and must never give up – in the correct exercise of the profession – the richness of direct communication". Moreover, the CNB expressed a set of problematic aspects concerning the use of the internet in healthcare, stressing that "without the doctor-patient direct relationship, it appears extremely difficult both collecting the informed consent and identifying the subject deontologically responsible for the information process." http://www.governo.it/bioetica/eng/pdf/ethics_health_and_new_information_tecnologies_20060421.pdf

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Medical treatment:	Is it allowed to perform medical treatment via online services? If yes, how should the medical services be provided? Does it have to follow the same requirements of a regular physically-present medical treatment?
	The national guidelines identify many services in the areas of remote monitoring and care ("telesalute" - real-time or asynchronous) interactions between patient and provider or among providers ("telemedicina specialistica"). No other information has been provided.
Medical data:	How should the data collected via a medical treatment performed online be processed? Are there specific requirements? Which ones?
	The data controller must comply with all data protection safeguards, including security requirements (see previous answers). Regions must develop an organizational structure and provide a specific framework to offer telemedicine services.

Other comments and technologies
Should you wish to describe any technology, feature or trend that has not been covered by the questionnaire, please feel free to use the space provided below. Where relevant, also indicate recent legislation changes, guidelines and/or case law.
-

IRELAND / IRLANDE

QUESTIONNAIRE

The questionnaire should ideally be completed by data protection authorities, health policy authorities, professional or patient associations as well as healthcare providers: you are invited to share it as widely as possible.

Please send your replies to dataprotection@coe.int no later than 15 December 2014.

1. Mobile Health (mHealth) and Electronic Health Records (EHR)

1.1. Data Protection Issues:

This is perhaps the biggest topic sitting at the intersection of technology and data protection. Mobile health (mHealth) and Electronic Health Records (EHR) are increasingly used in healthcare systems and provisions – it is a trend that needs to be examined.

Related to the EHR, these records are more accurate, cost-effective (in terms of storage) than paper-based notes. The concept of patient controlled/accessed EHR has been implemented in varying degrees in different countries.

Furthermore, some non-medical record can still contain health information about users and it should be considered if such records ought to be treated in a similar way to EHR.

Also, should 'medical data' as defined in Recommendation N° (97) 5 on the protection of medical data cover physical tracking data, such as pedometers or fitness data and data that can lead to medical information about an individual ?

1.2. Questions: if EHR exist in your country, is your legal framework providing for a regulation of such records? If mHealth exists in your country, is your legal framework providing for a specific regulation? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	With regard to EHR, the legal framework is Section 12 of Decree Law no. 179/2012 which, amongst others, sets forth the purposes of EHR, the bodies in charge of pursuing the different scopes, and the access requirements (based on data subject's consent). Please note that Section 12.2 explicitly refers to the data protection requirements provided for by the Italian Data Protection Code (legislative decree 196/2003, available, in English, at the following link: http://194.242.234.211/documents/10160/2012405/DataProtectionCode-2003.pdf) According to Section 12.7, the Ministry of Health must issue one or more decrees for the full implementation of section 12 of decree 179/2012. The adoption of the first implementation decree is forthcoming. According to Art. 12 of Decree Law no. 179/2012 the Electronic Health Record is defined "as a set of digital data and documents relating to health and social health clinical events generated by present and past, regarding the patient, which is intended to facilitate patient care, provide a service that can foster the integration of different skills, deliver a consistent information base, contributing to the improvement of all activities and nursing care, in compliance with the regulations for the protection of personal data". Activities have been planned for the implementation of Electronic Health Record systems at regional level. Decree Law no. 69/2013 established that consent or refusal for organ donation falls within the EHR (Article 43, paragraph 1a).

	Please note that our legal framework does not provide for a specific regulation of mHealth. However, the Data Protection Code applies in this sector too, including some specific provisions concerning data processing within electronic communication sectors (See Title X of the DPCode).
Case-law:	-
Other:	**EHR:** In respect of EHR, Guidelines on the Electronic Health Record and the Health File were adopted by the Italian Data Protection on 16 July 2009 (available in English at: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1672821) The Guidelines, which drew inspiration from the work of the Article 29 Working Party (see the Working Document adopted on 15 February 2007 http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp131_en.pdf), were issued by the DPA - pending at that time the enactment of specific legislation - following a public consultation that involved the relevant practitioners; They lay down a first set of rules to ensure the protection of medical data and safeguard individuals. Moreover, on 22 May 2014 the Italian DPA adopted an opinion on the first draft Decree implementing Decree 179/2012, which sets forth the information and documents to be included in the EHR, the responsibilities and tasks of the different entities/subjects involved, the data protection safeguards and security measures to be adopted, the criteria for accessing the EHR, and the interoperability criteria. The (favourable) Opinion is available (only in Italian) at: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3230826) **mHealth:** The Italian DPA participated in the second annual Global Privacy Enforcement Network (GPEN) Privacy Sweep, concerning apps. https://www.priv.gc.ca/media/nr-c/2014/nr-c_140910_e.asp Our DPA decided to focus on health apps. The results of the Italian sweeping activity showed that the degree of transparency on the processing of users' data and the permissions required to download the selected medical Apps, in some cases, are not in line with the Italian data protection legislation. 50% of App showed lack of "privacy pre-installation communications" (i.e. privacy policy prior to the App installation) or too general privacy policies or not tailored for the smart phone/tablet small screen, or even hidden in the credit section. As for Italian DPA's tasks, at the national level, the Authority is planning an assessment in terms of needed inspections and any possible prescriptive measures/sanctions. (See press release: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3375236)

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
EHR and Medical data:	What can be considered medical data in your country? Is it solely the data relating to a person's health (state, diagnosis, prognosis, medical treatment, etc.)? Is non-medical data that leads to medical information treated the same way as medical data (for instance in terms of confidentiality requirements)? Is the EHR solely constituted of data collected in a medical context or can the individual also himself or herself add information regarding his or her health?
	Definition of health data: According to Section 4, paragraph 1, letter d) of the DPCode, **personal data disclosing health** are "sensitive data" and therefore subject to specific safeguards (as provided for by Article 6 of Convention 108/1981 and Article 8 of Directive 95/46). Although there is not a definition of medical data in the DPCode, the concept of "personal data disclosing health" – which enjoy even stricter safeguards among sensitive data - is broad enough to cover all those data enabling the disclosure of health.

	For example, on several occasions the Italian DPA considered the information concerning the illness status in an employment sector (in case of absence for illness) to be health data. See in particular "Guiding Principles Applying to the Processing of Employees' Personal Data for the Purpose of Managing Employment Relations in the Private Sector" http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1427027, see Sections 5.3 and 6.1) and Guiding principles on the processing of employees' personal data in the public sector http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1693793 - See Section 6.3). Also the reference, associated to an individual, to a law providing for benefits for certain categories of people (such as people with disabilities) may fall under the notion of health data and be therefore subject to special protection. Please note that the European Data Protection Supervisor (EDPS) has focused on the concept of health data on several occasions. See for example: - "Guidelines concerning the processing of health data in the workplace by Community institutions and bodies" ("Health data generally refers to personal data that have link with the health status of a person. This would normally include medical data (e.g. doctor referrals and prescriptions, medical examination reports, laboratory tests, radiographs), as well as administrative and financial data relating to health (e.g. medical appointments scheduling, invoices *for healthcare service provision, indication of the number of days of sick leave, sick leave management"*). https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Supervision/Guidelines/09-09-28_Guidelines_Healthdata_atwork_EN.pdf - Opinion on the Communication from the Commission on 'eHealth Action Plan 2012-2020 - Innovative healthcare for the 21st century https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2013/13-03-27_eHealth_Action_EN.pdf - Opinion on the proposal for a directive of the European Parliament and of the Council on the application of patients' rights in cross-border healthcare https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2008/08-12-02_Crossborder_healthcare_EN.pdf **Additional data on EHR:** According to Section 5 of the said forthcoming first implementation decree (in application of the section 12 (7) of D.L. 179/2012), the individual can add information by herself/himself on a specific section of the EHR called "personal notebook".
Sharing of data and Access:	Who is granted access to the EHR and how is the sharing of information (with other health care providers?) regulated? Where information is shared with pharmacists, is there a strict purpose limitation in place? How has the definition of the responsibility over the medical data been regulated?
	According to Sections 10, 14, 18 and 21 of the said forthcoming first implementation decree of the Ministry of health, the following subjects are allowed to access the EHR: patient (data subject), Regions and Autonomous Provinces, Health Regional Services and Social-health Regional Services, Ministry of Health. According to Section 12 (2 bis) of D.L. 179/2012, the pharmacist will be allowed to access with the only purpose to view the medical prescriptions. The responsibility over the medical data is regulated according to Sections 28-30 of the DPCode. In respect of the role and responsibilities allocated on data controllers and processors, see also the abovementioned Guidelines on EHR issued by the Italian DPA

	http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1672821, in particular Section 2 and 4.
Data quality:	Are the principles of legitimacy, fairness and minimisation applied to medical data? How are records kept accurate? How long is the data kept for, is the specific storage period defined for the EHR?
	Legitimacy, fairness and minimisation are general data protection principles (Sections 3 and 11) that *a fortiori* apply to medical data. The data are updated each new healthcare performance, unless the data subject decides to obscure the information for any reason. The specific storage period for the EHR is not defined. Please note that in the said Guidelines (see previous answer) the DPA stated that if consent is withdrawn the EHR the medical records contained therein should be further available to the health care bodies that have drafted them (this applies, for instance, to the hospitalization information that may be used by the given hospital), without prejudice moreover to their retention where required under the law; however, they should no longer be shared among the other health care bodies/professionals treating the given data subject (Section 22(5) of the DP Code).
Data integrity:	Are any specific methods used to ensure the integrity of the data? How are patients identified in the EHR? In the context of research, are anonymisation methods used and what safeguards exist for re-identification?
	Data integrity (and security) The ongoing implementing decree provides for appropriate measures aiming at security and integrity of data such as: - authentication and authorisation systems applied to the persons in charge for the processing as a function of the respective access/processing requirement; - procedures to regularly check quality and consistency of authentication credentials and authorisation profiles applying to the persons in charge for the processing; - criteria to encrypt and/or keep separate the data suitable for disclosing health and sex life from any other personal data; - logging of accesses and operations; - audit logging to control database accesses and detect abnormalities; - secure communication protocols by implementing encryption standards for electronic data communications between the various data controllers. Such measures were contained in the said Guidelines on EHR adopted by the DPA in 2009. The said decree also provides for the obligation for the data controller to notify data breaches to the DPA. Such measure was also suggested by the DPA in its Opinion of 22 May 2014 on the draft decree http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3230826). **Identification of the patient:** In the EHR, the patient is identified with name, last name and tax code. The data required for the correct identification of the patient in feeding the EHR are listed in a Technical Annex of the decree. **Research** In the context of research pseudo-anonymisation methods are adopted. The specific safeguards provided for by the Code of conduct on processing of personal data for scientific and statistical purposes, attached to the DPCode, must be also ensured.
Data security:	Where are the records stored? Is there a centralised database of EHR? What security technology is being used?
	The records are stored from data controllers in their archives. There is not a centralized database of EHR. In respect of security, please see the previous answer.
Rights of the person/patient	How can the right of access be exercised? How can the data be corrected? Can the person enter information in his or her own EHR? What are the legal remedies available?
	Rights of access and correction can be both exercised according to the Section 7 of the DPCode.

concerned:	As mentioned before, the data subject is allowed to add data related to her/him on a specific section of the EHR. With regard to remedies, the rights as per Section 7 may be enforced either by filing a lawsuit or by lodging a complaint with the Garante. The DPA is not competent for compensation of damages (See Section 15 of the DPCode) which is left to the judicial competence. Remedies before the DPA are set forth by Section 141-151 (claims to point out an infringement of the relevant provisions on the processing of personal data; report to call upon the DPA to check up on the data protection provisions; complaints with a view to establishing the specific rights referred to in Section 7).
Consent:	Is the system based on an opt-in approach? Is the principle of granular consent applied (with the possibility of preventing access to certain data?)? If yes, in which situations?
	The system is based on an opt-in approach. The refusal to have an EHR should not affect the patient's right to medical care. The principle of the granular consent is applied. The patient can choose which information should be stored, from whom information can be viewed and whether to blank some information. A mechanism of “blank the blanking” is also provided, as also suggested by the DPA in the said Guidelines on EHR.
Withdrawal:	Are patients able to withdraw the consent given to EHR schemes? If yes, what is the relevant procedure to withdraw such consent? What are the consequences?
	The patients are always able to withdraw the given consent, according to the Section 8(6), of the forthcoming first implementation decree of the Ministry of health (in application of the section 12 (7) of D.L. 179/2012). There are no consequences for, as mentioned before, patient's right to medical care is guaranteed even in case of refusal or withdrawal to have an EHR.
Outsourcing processing of data:	Is outsourcing common? Under what circumstances? Where is the data outsourced to? What sort of safeguards are in place?
	None of the contributions to the questionnaire received refers to cases of outsourcing. In respect of its institutional activity related to EHR, the Italian DPA has not experienced any case of outsourcing so far.

2. Cloud Computing, Data Mining and Profiling from both Medical Records (including EHR) and Data not specifically related to medical records.

2.1. Data Protection Issues:

Cloud computing has brought a new dimension to the way data is stored, accessed and processed. Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS), Network as a service (NaaS) are all used by services and organisations that deal with both medical data and non-medical data.

With the development of more advanced and efficient data-mining and data-querying Medical techniques (e.g NoSQL, MapReduce, Hadoop) in conjunction with increased processing power and data storage, mining data has never been more informative, easier, and cost-effective.

Healthcare is a natural sector in which to apply new technologies and methodologies, with particular impacts in epidemiology, public health, health services research, etc.

Data that can lead to the identification of a particular individual and his/her health situation is not limited to medical data *per se,* present on Electronic Health Records, but also to unsuspicious type of information.

There is a growing concern that these schemes may be implemented in manner which does not always respect the patients’ confidentiality and basic rights, and in a broader context, the use of this

of information may prejudice the individuals concerned. The ability to track and monitor patients and resources enables a more efficient provision of care but may have an impact on the right to privacy of the individual concerned.

2.2. Questions: Is your legal framework providing for a regulation of Cloud Computing, Data Mining and Profiling? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	**Cloud computing**: There is not a specific legal specific framework for cloud computing. However, data protection principles, as provided for by the DPCode, should apply as in any other sector. **Profiling**: A specific provision of the DPCode concerns "Profiling of Data Subjects and Their Personality" (Section 14). According to such provision, no judicial or administrative act or measure involving the assessment of a person's conduct may be based solely on the automated processing of personal data aimed at defining the data subject's profile or personality. Moreover, the data subject may challenge any other decision that is based on such kind of processing.
Case-law:	-
Other:	As regards cloud computing, the Italian DPA decided to issue a "mini-vademecum" called "Cloud Computing – Protect Your Data without Falling from a Cloud". The vademecum, which concerns cloud computing in general and not only the health sector, includes specific examples and a Decalogue with practical tips and suggestions for further analysis. http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1906181 Data mining and Profiling were considered by the DPA on several occasions (prior checking under Section 14 and 17 of the Code) although more in connection with the tlc sector, electronic communications and marketing. Please note that with a Decision of 7 December 2006 the DPA dealt with a case where personal data related to pregnant women, in neonatal health facilities or clinics, were collected - for marketing purposes - by a publisher of a review on childhood, with the help of the personnel of the clinic who received gifts and benefits from the publisher. With that decision, the DPA prohibited the processing which had been carried out in violation of several DPCode provisions, including transparency obligations, designation of controller/processor, and exercise of data subject's rights. See http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1379101

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Cloud computing:	How is cloud computing regulated in your country? Which security safeguards and standards are mandatory? Are there specific requirements in order to store medical data in the cloud? How is data shared and is the sharing regulated?
	See previous answers.
Government:	Do governmental programmes exist to allow for increased data-mining of medical records? If yes, what are the purposes of this data mining? Are private entities allowed to access the data? Under what circumstances? What sort of techniques and technologies are being used? To what end? Are data subjects informed of this type of data-mining?
	In the Ministry of Health, the New Health Information System (NSIS) is the

	information system dedicated to governance purposes. Data-mining initiatives are still in an early phase of scope definition. The law provides for the possibility to interconnect health records at national level but only by using unique codes related to patients.
Private sector:	Are private entities allowed to mine medical data which they process? Under what circumstances? Can the government have access to this data?
	Private entities can mine medical data obtaining the consent from data subject or using irreversibly anonymized data. The government can access to this data, in aggregated form, and only for health quality assessment purposes.
Profiling:	Are the government and the private sector allowed to employ profiling methods on medical data? If yes, under what circumstances? Is it allowed to cross and correlate non-medical data with medical data?
	For any cross connection, correlation or profiling activity, the general legal framework applies. The scope of treatments in the public sector does not include profiling for governance purposes. A specific regulation for a comprehensive cross-connection among different medical information in NSIS is ongoing.

3. RFID and wireless communication technologies

3.1. Data Protection Issues:
It is common for medical devices, such as patients' tags, to possess RFID technologies in order to facilitate the transmission of the patients' data.
It can also be related to the data-mining operations previously mentioned as it is another category of information that can be used to discern meaningful patterns.

Transmission of data through radio-frequency is not limited to medical devices. Almost any smartphone uses some technology enabling to collect, and share, the user's data. For instance, via WI-FI it is possible to identify users' locations and therefore infer some of their behaviour, which in some cases can relate to health information.

3.2. Questions: Is your legal framework providing for a regulation of RFID technologies and the transfer of personal data through wireless technologies? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	Italy does not have a specific legal framework for RFID technologies and the transfer of personal data through wireless technologies. Data protection requirements, as provided for by the DPCode, apply in this sector too.
Case-law:	-
Other:	On 9 March 2005, the DPA adopted a general decision setting forth the specific safeguards to be put in place while processing data through the use of RFID: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1109493 Moreover, with a decision adopted 29 November 2012 following a prior checking request (Section 17 of the DPCode), the DPA dealt with the processing of personal data through RFID for the remote monitoring of patients with implantable cardiac defibrillators. The DPA prescribed to both the hospital and the producer of the RFID device adequate measures to be adopted in order to ensure the full compliance with the DPCode. (data subject's consent, possibility for an easy deactivation of the remote control device, stringent data security measures, specific safeguards for the outsourcing of certain activities regarding security checks on the said devices). http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2276103

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
RFID:	How is RFID used in hospital/clinics for (a) resource management, (b) patient care? What types of database systems (and security) are implemented in conjunction with RFID use? How are issues of access, sharing, consent etc. managed considering that RFID may be used without the patients' knowledge.
	No information was provided regarding this issue.
Wireless tracking technologies:	Are hospitals/clinics employing other wireless tracking technologies besides RFID? Which ones? Do they have to follow specific security requirements? Which ones?
	No information was provided regarding this issue. In respect of security requirements see the abovementioned decisions by the DPA, respectively of 9 March 2005 and 29 November 2012.

4. Applications (Mobile)

4.1. Data Protection Issues:

Information society is increasingly relying on the use of "apps" (application), most of them mobile. These apps are commonly designed to gather personal data, and in practice often process medical data.
Technologies such as multi-touch touchscreen, accelerometers or gyroscopes, ambient light sensors, GPS and cameras, and devices featuring fingerprint and biometric sensors also involve the collection of medical data.
A mobile phone application can monitor accurately physiological data, such as heartbeats, sleep patterns, fitness information.

4.2. Questions: Is your legal framework providing for a regulation of Apps and Mobile Apps? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	There is not a specific regulation concerning Apps and Mobile Apps. Nevertheless, the processing of data in this field should be carried out in the due respect for data protection principles as set forth by the DPCode.
Case-law:	-
Other:	As stated before, the Italian DPA, following the Sweep initiative, announced inspections and possible prescriptive measures/sanctions concerning the processing of data related to medical apps. The DPA actively took part in the elaboration of the Article 29 Working Party's Opinion 2/2013 on apps on smart devices http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Apps:	Is it allowed to use apps and mobile apps to deploy medical services and collect medical data? If yes, which type of individual/organisation can develop and employ these apps? Are there specific security requirements for these types of apps?
	Yes, it is allowed to use apps and mobile apps to deploy medical services and collect medical data but the data controller must comply with the current legal framework, including data protection requirements. In order to answer to this and the following questions regarding security

	requirements, it is important to consider that there are several subjects intervening in the processing of data related to the use of apps ("app developers", including "app owners", "app stores", etc.) who are called upon to ensure fulfillment of DP requirements. The roles and responsibilities of the different subjects involved, in particular concerning security measures has been analysed by the Article 29 Working Party in the said Opinion 3/2013 to which we refer to (See in particular section 3.3. and 3.7 of the Opinion)
Institutions:	Do hospitals/clinics/labs employ apps to gather medical data? Is there a need for a medical treatment to permit the use of an app to process the medical data? Are there specific security requirements for the institutions collecting these data from the apps? Are medico-administrative data used by hospitals/clinics for management purposes?
	No specific answers were provided on the employment of apps in hospital/clinics/labs. Hospital/clinic/labs must respect the security requirements provided for by Sections 31-36 of the DPCode, including the specific safeguards in case of processing of data disclosing health performed by health care bodies by electronic means (encryption techniques or identification codes. see Section 34, para 1, lett. h). Please note that technical specifications concerning minimum security measures are contained in the Annex B of the DPCode, including in respect of the processing carried out by health care bodies and professionals on data disclosing health and sex life. Medical-administrative data could be used by hospitals/clinicsfor management purposes always in the due respect of data protection principles.
Tracking technologies:	Do hospitals/clinics/labs employ non-medical apps and devices to track and collect data from their patients? What type of data is collected? For what purpose? Is the data identifiable? Is the data combined with medical data?
	No information has been provided on this issue
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical apps and tracking apps? If yes, what are the standards?
	Although there is not a specific privacy by design requirement for medical and tracking apps, Section 3 of the DPCode, which applies to data processing in any sector, states that information systems and software must be configured by minimising the use of personal data and identification data, in such a way as to rule out their processing if the purposes sought in the individual cases can be achieved by using either anonymous data or suitable arrangements to allow identifying data subjects only in cases of necessity, respectively.
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical diagnostic? How would this be applied to fitness and daily-basis data?
	The system should be based on opt-in. The collection of data should be justified by medical purposes (such as prevention, diagnosis, treatment, etc.). Generally speaking, the DPCode requires the data subject's (written) consent for any processing of health data (online "clicking" is considered to be equivalent to a written consent). Such rule would be applied also to fitness and daily-basis data as long as such data disclose information on the individual's health.

5. Medical Devices and Wearable Devices

5.1. Data Protection Issues:

A medical device can be defined as: 'any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application. Such a device should be intended by the manufacturer for one of a number of defined purposes, one of which is, diagnosis, prevention, monitoring, treatment or alleviation of disease' (Directive 93/42/EEC Article 1:2) Some eHealth and mHealth devices and apps do not fall in this definition of medical devices, as can also be the case of a software working in combination with a physical device, for instance a smartphone.

5.2. Questions: Is your legal framework providing for a regulation of Medical Devices? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	Yes, the Italian legal framework provides for the regulation of medical device or in-vitro device according the Directive 93/42/EEC concerning medical devices (Legislative Decree 24 February 1997 no 46 http://www.salute.gov.it/imgs/C_17_normativa_515_allegato.pdf) and Directive 98/79/EC on in vitro diagnostic medical devices (Legislative Decree September 2000, no. 332 http://www.salute.gov.it/imgs/C_17_normativa_544_allegato.pdf)
Case-law:	-
Other:	-

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
General answer: On 26 September 2012, the European Commission adopted two Proposals, one for a Regulation on medical devices and the other for a Regulation on in vitro diagnostic medical devices which, once adopted, will replace the existing legal framework applicable to medical devices in EU. There are no binding rules in EU as to the difference between lifestyle and wellbeing apps and a medical device or in vitro diagnostic medical device. Since January 2012, in order to help software developers and manufacturers identify whether their products fall or not under the Directive on medical devices or the Directive on in vitro diagnostic medical devices, the Commission's services issued some guidance which will be continuously updated (Guidelines on the qualification and classification of stand-alone software used in healthcare within the regulatory framework of medical devices, MEDDEV 2.1/6 January 2012). These Guidelines are, at the moment, the only legal framework for app and software used in healthcare.	
eHealth and mHealth:	Does the concept of Medical device in your country encompass services and apparels in the realm of eHealth and mHealth? What are the requirements? Should, for instance, the medical device be certified before it can be used?
	See the previous answer
Apps:	Does the concept of medical devices encompass apps? If yes, is there any regulation applicable to apps that perform medical services? Is there any regulation applicable on apps that track non-medical data that can lead to health information? If yes, what type of data?
	See the previous answer
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical and/or wearable devices? If yes, what are the standards?
	See, as per answer 4.2, Section 3 of the DPCode.
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical treatment? How would this be applied to fitness and

	daily-basis data?
	See answer 4.2

6. Internet of Things

6.1. Data Protection Issues:

Internet of things relates to common, ordinary devices that are now, and increasingly, connected to the Internet, such as cars, fridges, ovens, microwaves, etc. All of these devices can provide data that can lead to reveal information concerning one's health. A fridge can easily inform on the type of food stored and thus the diet of an individual. One of the biggest challenges of the Internet of Things is to guarantee the right to privacy and data protection in a world where every device collects, processes, analyses and transmits the data, commonly via wireless technologies.

In the realm of medical data, the issue mainly arises when crossing seemly unrelated data that can lead to health information about an individual.

6.2. Questions: Is your legal framework providing for a regulation of the Internet of Things? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	There is not a specific legal framework providing for internet of things. As in any other sector the DPCode should apply.
Case-law:	-
Other:	-

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Security:	What are the security standards that need to be employed by these devices when collecting personal data?
	In respect of data security, the requirements provided for by the DPCode should apply.
Non-medical devices:	Are non-medical devices allowed to collect medical data, such as heart frequency? Are they allowed to cross medical data with non-medical data?
	No information has been provided on this issue.
Privacy by Design:	Is there any requirement to implement privacy by design in the development of connected devices? If yes, what are the standards?
	Again see Section 3 of the DPCode, which applies to any sector.

7. Electronic Doctor (online Doctor) and on-line appointments

7.1. Data Protection Issues:

The Doctor listens, talks and assesses the patient online, via a website, app, canal, sometimes including video-conference. Medical data is collected and processed, what are the security requirements and standards followed? Other websites provide for on-line appointments with doctors, which can also involve the processing of medical data.

7.2. Questions: Is your legal framework providing for a regulation of online Medical Treatment and is the on-line appointment system covered by such a framework? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	The Ministry of the Health set up within the National Health Council (CSS), a working group for Telemedicine. The working group is composed of members and experts of the CSS, General Managers and representatives of the Ministry of Health. This working group defined specific national guidelines ("Telemedicina, linee di indirizzo nazionali") which have been adopted with a State-Regions agreement on February 20, 2014. http://www.salute.gov.it/imgs/C_17_pubblicazioni_2129_allegato.pdf There are also few regional laws on telemedicine. Again, the general data protection legislation is the DPCode.
Case-law:	-
Other:	Please note that on 25 January 2012 the DPA issued "Guidelines on processing personal data for dissemination and publication on exclusively health-related web sites". Such guidelines refer to the processing of personally identifying and/or sensitive data relating to users on exclusively health-related web sites – where one can ask for advice, exchange information, and share comments. The guidelines point out the safeguards to be adopted so that such processing is performed in compliance with personal data protection legislation, in particular, by ensuring that the data in question are relevant and not excessive and that they are processed fairly and in good faith (see section 11 of the Code): http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1879894 The Italian National Bioethics Committee (CNB) issued an Opinion on Ethics, Health and New Information Technologies (21st of April 2006), whereby recommending that "in the training of a doctor, specialist and healthcare personnel, it will be important to insist also on ethico-legal problems concerning the protection of "privacy" and caution in the preservation, processing and transmission via the internet etc. of the patient's health data, according to international and national binding regulations. The doctor and in general the health operator, when required and interested in professional communication on the internet, must, deontologically, keep sight of the "human" complexity of the doctor/patient relationship and must never give up – in the correct exercise of the profession – the richness of direct communication". Moreover, the CNB expressed a set of problematic aspects concerning the use of the internet in healthcare, stressing that "without the doctor-patient direct relationship, it appears extremely difficult both collecting the informed consent and identifying the subject deontologically responsible for the information process." http://www.governo.it/bioetica/eng/pdf/ethics_health_and_new_information_tecnologies_20060421.pdf

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Medical treatment:	Is it allowed to perform medical treatment via online services? If yes, how should the medical services be provided? Does it have to follow the same requirements of a regular physically-present medical treatment?
	The national guidelines identify many services in the areas of remote monitoring and care ("telesalute" - real-time or asynchronous) interactions between patient and provider or among providers ("telemedicina specialistica"). No other information has been provided.
Medical data:	How should the data collected via a medical treatment performed online be processed? Are there specific requirements? Which ones?
	The data controller must comply with all data protection safeguards, including security requirements (see previous answers). Regions must develop an organizational structure and provide a specific framework to offer telemedicine services.

Other comments and technologies
Should you wish to describe any technology, feature or trend that has not been covered by the questionnaire, please feel free to use the space provided below. Where relevant, also indicate recent legislation changes, guidelines and/or case law.
-

MONACO

DOCUMENT DE TRAVAIL

QUESTIONNAIRE – MISE A JOUR DE LA RECOMMANDATION 97-5

1.1 L'expression « données médicales », au sens de la Recommandation 97-5 relative à la protection des données médicales, doit-elle inclure les données personnelles recueillies par un procédé de localisation / détection électronique, à l'instar d'un podomètre, ou des données personnelles afférentes à un exercice sportif ou d'autres données pouvant conduire (indirectement) à des données médicales sur la personne ?

L'extension du champ d'application de la Recommandation 97-5 se pose effectivement à l'aune de la collecte de données médicales ou de santé hors contexte médical au sens traditionnel du terme. Une telle extension aurait nécessairement un impact sur la législation applicable, les données ainsi collectées passeraient du régime applicable aux données personnelles, qui constitue le droit commun, à celui plus spécifique des données de santé, renforçant ainsi les obligations applicables et, corrélativement, la protection des droits des personnes.

De manière générale, on peut considérer que le droit est désormais confronté, par l'évolution des nouvelles technologies, à la nécessité d'appréhender des données qui, de par le contexte dans lequel elles sont recueillies, peuvent perdre leur caractère de données médicales. On aboutirait, schématiquement, à un triptyque dont les éléments de classification dépendraient précisément du contexte dans lequel la collecte des données viendraient s'inscrire, c'est-à-dire, le contexte médical, le contexte sportif et un contexte plus personnel.

Pour ce dernier cas, il est important de noter que la sollicitation à laquelle se trouve confrontée la personne s'inscrit aussi dans une logique à la fois consumériste et d'épanouissement personnel, les données recueillies pouvant être considérées comme des données de « bien-être ». Ainsi, plus que l'extension de la notion de données médicales, la question de l'élaboration d'une législation autonome couvrant ces différentes matières, en lien avec la protection des informations nominatives, pourrait constituer, dans un futur proche, un nouveau défi pour les Etats.

1.2 Si votre Pays fait usage ou a recours à des dossiers médicaux électroniques, existe-t-il un cadre légal prévu à cet effet ? Même question s'agissant de la « Santé Mobile » c'est-à-dire l'utilisation de la technologie Smartphone / Tablette à des fins de solutions de santé ou d'information en matière de santé. Dans la négative, comment le droit commun de la protection des données peut-il être appliqué pour couvrir ces domaines ? Indiquer les textes, jurisprudence, normes ou recommandations pertinents en la matière.

Il n'existe pas à Monaco de dossier médical électronique unique qui retracerait l'ensemble des actes et prestations de soins délivrés au patient durant toute sa vie. La Principauté n'a pas mis en place de dossier médical partagé.

En revanche, afin d'assurer le suivi médical de leurs propres patients, les professionnels de santé peuvent, bien entendu, tenir leur dossier médical sur un support électronique et utiliser des techniques automatisées de gestion des dossiers des patients et des assurés sociaux.

Toutefois, il n'existe pas de cadre juridique spécifique à ces dossiers médicaux électroniques ou à l'utilisation de la technologie Smartphone / Tablette à des fins de solutions ou d'informations en matière de santé, ni, d'ailleurs, aux progiciels et aux applications mobiles, lesquels demeurent néanmoins soumis aux règles du droit commun, notamment à celles de protection des informations nominatives.

Aussi, et du fait de la nature des données collectées, la loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives a vocation à s'appliquer et le régime applicable dépendra de la caractérisation de la nature des données en présence.

Ainsi, le principe posé par l'article 12 de la loi n° 1.165 précité reste l'interdiction, laquelle est alors assortie d'exceptions limitativement énumérées et qui tiennent :

- au consentement écrit et exprès de la personne concernée qui doit pouvoir à tout moment, revenir sur son consentement et solliciter du responsable ou de l'utilisateur du traitement la destruction ou l'effacement des informations la concernant ;

- au motif d'intérêt public ;

- à la finalité : médecine préventive, diagnostics médicaux, administration de soins, médications ou gestion des services de santé et de prévoyance sociale, ou dans l'intérêt de la recherche, si le traitement est effectué par un praticien de la santé ou par une autre personne soumise à une obligation de secret ;

- lorsque le traitement porte sur des informations manifestement rendues publiques par la personne concernée ;

- lorsque le traitement est nécessaire à la constatation, à l'exercice ou la défense d'un droit en justice ou répond à une obligation légale.

Les questions relatives aux dossiers médicaux et à la santé mobile sont donc examinées sous cet angle par l'autorité nationale de contrôle du respect des informations nominatives, c'est-à-dire la Commission de Contrôle des Informations Nominatives (ci-après CCIN).

La CCIN a indiqué ne pas avoir été sollicitée, à ce jour, sur la mise en œuvre d'applications mobiles en lien avec la santé ou le bien-être.

La CCIN relève en outre que ces applications soulèvent toutefois la question de l'utilisation domestique d'applications électroniques comportant des données à caractère personnel, de traitement d'informations personnelles, par la personne concernée elle-même qui viendrait, si elle le souhaite, à partager ses informations avec des tiers, de la sorte à les rendre publiques sur des forums, des sites de partage ou autres.

Dans le premier cas, la question de l'applicabilité des principes de la loi aux traitements réalisés à l'aide des applications se pose réellement car il pourrait être considéré que ces utilisations relèvent « *des activités personnelles ou domestiques* » des personnes concernées. Dans ce cas, l'utilisation de ces applications sortirait du champ d'application de la loi n° 1.165 (art.24-2 chiffre 3).

Les développeurs et les personnes qui mettent sur le marché (au sein de plate-forme de mise à disposition d'application) ces outils s'inscrivent souvent dans cette logique. Ils mettent à disposition des outils de « coaching » personnel à utiliser à des fins personnelles dans le cadre d'activité personnelle. L'accompagnement est individualisé si la personne le souhaite.

Dans le second cas, le traitement des données est opéré dans le cadre d'une exception à l'article 12 puisque les informations ont été « *manifestement rendues publiques par la personne concernée* » donc en toute légalité au sens de la loi sur la protection des informations nominatives.

1.3 Que recouvre la notion de données médicales pour votre Pays ? Cela concerne-t-il uniquement les données relatives à la santé d'une personne (son état, diagnostic, pronostic, traitement médical, *etc.*) ? Les données non-médicales pouvant conduire à l'obtention d'informations médicales font-elles l'objet d'un traitement similaire aux données médicales proprement dites ? Le dossier médical électronique est-il uniquement composé de données recueillies

dans un contexte médical ou le patient peut-il compléter ou ajouter des informations relatives à sa santé ?

Il n'existe pas, dans l'ordonnancement juridique monégasque, de définition de la notion de données médicales. Les trois premières questions sont donc sans objet.

Toutefois, il est intéressant de noter que, lors de la modification de la loi relative à la protection des informations nominatives en 2008, les terminologies ont été changées. En effet, jusqu'en 2008, la loi visait aux « informations à caractère médical » et, à partir de 2008, les données de santé, y compris les données génétiques.

Néanmoins, le législateur n'a pas défini la notion de « données de santé ». Il a simplement mentionné qu'il s'agissait d'une « *notion plus large ».* Aussi, à partir du moment où des informations sont susceptibles de faire apparaître, directement ou indirectement, des données de santé, la CCIN s'assure que les dispositions de l'article 12 de la loi sont respectées.

Celle-ci a d'ailleurs soulevé cette question dans son rapport d'activité 2013 (p. 57 et 58). Elle tient compte des documents du Comité européen d'éthique et de la jurisprudence des juridictions de l'Union européenne et de la Cour européenne des droits de l'homme pour déterminer la nature des données.

En outre, il est à noter que le premier alinéa de l'article 44 du Code de déontologie médicale prévoit que le dossier médical que le médecin doit établir pour chacun de ses patients « *comporte les informations dont il dispose sur la santé du patient, nécessaires aux décisions diagnostiques et thérapeutiques* ». Dès lors, force est de constater que ce texte vise toute information portant sur la santé d'une personne sans faire aucune distinction selon son caractère médical ou non-médical.

S'agissant de l'interrogation relative au dossier médical électronique, et en l'absence de dossier médical électronique unique, il appartient aux professionnels de santé concernés d'offrir ou non à leurs patients la possibilité de compléter leur dossier médical. Il semble que de tels procédés ne soient pas encore très développés dans un strict cadre médical et, qu'en pratique, seuls certains professionnels de santé exerçant dans le milieu sportif de haut niveau aient initié une telle démarche à l'égard des dossiers des sportifs qu'ils traitent.

1.4 Qui dispose de l'accès aux dossiers médicaux électroniques et comment est organisé le partage des informations, notamment avec les autres professionnels de santé ? Pour le cas où l'information serait partagée avec les pharmaciens, existe-t-il une finalité strictement limitée pour ce faire ? Quels sont les critères régissant la responsabilité en matière de données médicales ?

En l'absence de cadre juridique spécifique au dossier médical électronique, l'accès à ce dernier est régi par le droit commun, savoir d'une part, les règles relatives au droit au respect de la vie privée et au secret médical et, d'autre part, la loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives et l'Ordonnance Souveraine n° 2.230 du 19 juin 2009 qui en fixe les modalités d'application. Ainsi, l'accès au dossier médical tenu par un professionnel de santé pour son patient est limité à ce professionnel, audit patient et au médecin désigné à cet effet par le patient.

S'agissant du partage d'informations entre professionnels de santé, y compris avec les pharmaciens, le premier alinéa de l'article 64 du Code de déontologie médicale prévoit seulement que « *lorsque plusieurs médecins collaborent à l'examen ou au traitement d'un malade, ils doivent se tenir mutuellement informés ; chacun des praticiens assume ses responsabilités personnelles et veille à l'information du malade* ».

Subséquemment, il est possible de considérer que lorsque deux ou plusieurs professionnels de santé prennent en charge un même patient, ce qui suppose, en principe, le consentement préalable de ce dernier à chacune de ces prises en charge, lesdits professionnels peuvent échanger des informations relatives à leur patient commun, sauf opposition de celui-ci, et ce, afin d'assurer la continuité des soins ou de déterminer la meilleure prise en charge sanitaire possible. En revanche, l'un de ces professionnels de santé ne peut accéder au dossier médical de son patient tenu par un autre de ces professionnels s'il n'a pas été désigné à cet effet par son patient.

Il est à noter que, s'agissant des professionnels de santé exerçant à titre libéral, la CCIN, dans un avis n° 2010-14 du 3 mai 2010, a posé les bases d'une norme permettant la mise en œuvre de déclarations simplifiées dans le domaine de la gestion des dossiers des patients. Cette dernière a par ailleurs été concrétisée par un Arrêté Ministériel n° 2013-200 du 11 avril 2013, lequel évoque la possibilité d'un partage d'informations entre praticiens libéraux, qui s'inscrit toutefois dans le respect des règles susmentionnées.

1.5 Les principes de légitimité, proportionnalité et de minimisation s'appliquent-il aux données médicales ? Comment les dossiers sont-il maintenus à jour ? Quels sont les durées de conservations des données médicales et existe-t-il une durée de stockage/conservation propre aux dossiers médicaux électroniques ?

Les principes ci-dessus énoncés paraissent être des principes généraux du droit de la protection des informations nominatives. Aussi s'appliquent-ils logiquement aux données médicales.

Pour ce qui est de la conservation des données médicales, celle-ci varie au cas par cas, en fonction de la finalité des traitements d'informations nominatives déclarés ou autorisés. Il n'existe en effet pas de cadre juridique uniforme en la matière.

1.6 Des méthodes spécifiques sont-elles utilisées pour préserver l'intégrité des données ? Comment les patients sont-ils identifiés dans les dossiers médicaux électroniques ? Dans l'hypothèse de recherches, est-il fait usage de procédés d'anonymisation et quels sont les procédés de sauvegarde des données afin de permettre une identification ultérieure des patients dont les données ont été anonymisées ?

Les dispositions de l'article 1163-1 du Code civil, introduite par la loi n° 1.383 du 2 août 2011relative à l'économie numérique, pose, au titre la force probatoire de l'écrit électronique, la nécessité que celui-ci soit établi et conservé dans des conditions de nature à en garantir l'intégrité, ce qui invite les opérateurs à se prémunir contre les altérations qui pourraient affecter leurs données électroniques et à préférer la mise en œuvre de supports durables.

S'agissant des modalités d'identification des patients au sein des dossiers médicaux électroniques, celles-ci peuvent comprendre, en pratique, le nom patronymique, éventuellement le nom d'usage, le prénom, le sexe, la date de naissance, une reconnaissance phonétique et un scoring.

En application de l'article 7-1 de la loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives, tout traitement automatisé d'informations nominatives ayant pour fin la recherche dans le domaine de la santé est soumis au contrôle de la Commission de Contrôle des Informations Nominatives, lequel porte notamment sur les procédés d'anonymisation des données retenus.

Ainsi, dans le domaine de la recherche, les patients ne sont pas identifiables directement et un code alphanumérique leur est attribué. Le médecin investigateur disposera des éléments permettant de faire le lien entre le patient et le code, à l'aide d'un tableau établi sur support papier auquel il peut seul avoir accès et qui sera, une fois l'étude terminée, archivé avec les autres documents sous enveloppe scellée.

1.7 Où sont conservés les dossiers médicaux électroniques ? Existe-t-il une base de données centralisée ? Quel procédé technologique de sécurisation est utilisé ?

La conservation des dossiers électroniques est faite de manière individualisée par chaque établissement ou professionnel de santé. Il n'existe pas de bases de données centralisées de données médicales.

1.8 Comment le droit d'accès s'exerce-t-il ? Comment les données peuvent-elles être modifiées ? La personne peut-elle interagir directement avec son dossier médical électronique ? Quelles sont les voies de recours disponibles ?

D'un point de vue général, s'agissant du droit d'accès et de modification, celui-ci s'exerce dans le cadre prévu par la loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives et de l'Ordonnance Souveraine n° 2.230 du 19 juin 2009 prise pour son application. D'un point de vue pratique, il appartient au responsable du traitement de déterminer, dans le respect de ladite loi, les modalités de mise en œuvre du droit d'accès et de modification.

Concernant la possibilité d'interaction directe du patient avec son dossier médical électronique, il appartient, en l'absence de dossier médical électronique unique, aux professionnels de santé d'offrir ou non cette possibilité à leurs patients. En pratique, il est toutefois peu probable que les systèmes informatiques utilisés pour gérer les dossiers médicaux offrent une telle faculté.

Quant aux voies de recours disponibles, il s'agit, outre celles naturellement ouvertes devant les juridictions étatiques compétentes pour en connaître, de la possibilité pour toute personne dont les droits conférés par la loi n° 1.165 du 23 décembre 1993 ou les textes pris pour son application ont été méconnus, ou celle ayant des raisons de présumer que ces droits ont été méconnus, de saisir le président de la Commission de Contrôle des Informations Nominatives.

1.9 Le procédé repose-t-il sur l'adhésion de la personne concernée ? Le consentement est-il « granulaire » c'est-à-dire repose-t-il sur un système de blocage ponctuel de l'accès à certaines catégories de données ? Si oui, dans quelles situations ?

Sans objet.

1.10 Les patients peuvent-il retirer le consentement donné pour la mise en place de dossiers médicaux électroniques ? Si oui, quelle est la procédure ? Quelles en sont les conséquences ?

Sans objet.

1.11 Est-il fréquent d'avoir recours à un procédé d'externalisation de traitement des données ? Dans quelles circonstances ? Vers où les données sont-elles externalisées ? Quelles sont les mesures de sécurité mises en place ?

La législation monégasque n'interdit pas de procéder à l'externalisation des données médicales, dès lors que sont respectées les dispositions de l'article 17 de la loi n° 1.165 du 23 décembre 1993.

2.2 Existe-t-il un cadre juridique spécifique applicable au « cloud computing », « data mining » et « profiling » ? Dans la négative, comment le droit commun de la protection des données peut-il être appliqué pour couvrir ces domaines ? Indiquer les textes, jurisprudence, normes ou recommandations pertinents en la matière.

Les principes généraux posés par la loi n° 1.165 relative à la protection des informations nominatives s'appliquent aux données de santé. Lorsque celles-ci peuvent être traitées (cf. question 1), alors l'exploitation des données devra respecter lesdits principes.

Aucune disposition spécifique au « Cloud Computing », « data mining » et « profiling » n'est prévue en droit monégasque.

Les dispositions de la loi n° 1.165 relative à la protection des informations nominatives sont applicables aux traitements des données réalisés par ce biais, particulièrement, les articles 17 et suivants portant sur la sécurité des données.

Ainsi, le responsable de traitement (établissement de soin, professionnel de santé) devra s'assurer que les moyens technologiques qu'ils décident d'utiliser comporteront *: « des mesures techniques et d'organisation appropriées pour protéger les informations nominatives contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions d'informations dans un réseau, ainsi que contre toute autre forme de traitement illicite.*

Les mesures mises en œuvre doivent assurer un niveau de sécurité adéquat au regard des risques présentés par le traitement et de la nature des données à protéger.

Lorsque le responsable du traitement ou son représentant a recours aux services d'un ou plusieurs prestataires, il doit s'assurer que ces derniers sont en mesure de satisfaire aux obligations prescrites aux deux précédents alinéas.

La réalisation de traitements par un prestataire doit être régie par un contrat écrit entre le prestataire et le responsable du traitement ou son représentant qui stipule notamment que le prestataire et les membres de son personnel n'agissent que sur la seule instruction du responsable du traitement ou de son représentant et que les obligations visées aux deux premiers alinéas du présent article lui incombent également.

Si le prestataire souhaite avoir recours aux services d'un ou de plusieurs sous-traitants pour l'exécution de tout ou partie des prestations prévues au contrat susvisé, les dispositions de l'alinéa précédent s'appliquent à ces derniers ».

L'externalisation au travers d'un Cloud imposera donc des mesures de prévention particulières : l'adéquation du niveau de sécurité devra tenir compte de ce facteur et des risques présentés par l'absence de maîtrise des outils choisis.

L'exploitation des données ou le data mining devra également respecter les dispositions de la loi n° 1.165 du 23 décembre 1993, à commencer par la détermination de la finalité de l'exploitation des données, la licéité de cette exploitation, ainsi que les qualités de l'exploitant pour agir.

On relèvera que les données contenues dans les dossiers médicaux ne sont pas des données publiques. Le professionnel de santé, particulièrement le médecin, est responsable du dossier médical de son patient et doit s'assurer que les données qui lui sont confiées seront exploitées dans le respect de la législation.

De plus, les dispositions de l'article 44 du Code de déontologie médicale précisent que « *Le médecin doit tenir pour chaque patient un dossier médical qui lui est personnel : ce dossier est confidentiel et comporte les informations dont il dispose sur la santé du patient, nécessaires aux décisions*

diagnostiques et thérapeutiques. Dans tous les cas ces informations sont conservées sous la responsabilité du médecin. Tout médecin doit, à la demande du patient ou avec son consentement, ou aux médecins que le patient entend consulter, les informations et documents utilisés à la continuité des soins. »

Il convient également de relever que les métiers de la santé font l'objet de législations et réglementations spécifiques en Principauté et que seules les personnes autorisées à exercer pourront mettre en œuvre un dossier patient.

En l'état de la législation en Principauté, les données issues des dossiers médicaux sont protégées par le secret médical. Le « partage » de ses informations à des fins de data mining ou de profilage doit être autorisé par la loi.

Cette conception se retrouve à l'article 14-1 de la loi n° 1.165 qui dispose que : *« Toute personne a le droit de ne pas être soumise à une décision produisant des effets juridiques à son égard ou l'affectant de manière significative, prise sur le seul fondement d'un traitement automatisé d'informations destiné à définir son profil ou à évaluer certains aspects de sa personnalité.*

Une personne peut toutefois être soumise à une décision mentionnée au précédent alinéa si cette décision :

- *est prise dans le cadre de la conclusion ou de l'exécution d'un contrat, à condition que la demande de conclusion ou d'exécution du contrat, introduite par la personne concernée, ait été satisfaite ou que des mesures appropriées, telles que la possibilité de faire valoir son point de vue et de voir réexaminer sa demande, garantissent la sauvegarde de son intérêt légitime ;* [ce peut être le cas lorsque la procédure de profilage est initiée dans le cadre d'un contrat de crédit ou d'une assurance santé] *;*

- *« ou est autorisée par des dispositions légales ou réglementaires qui précisent les mesures garantissant la sauvegarde de l'intérêt légitime de la personne concernée »* [ce peut être le cas pour l'attribution de logement sociaux, des procédures d'accompagnement sociales liés à la santé, aux handicaps ou aux difficultés temporaires ou permanent d'une personne].

2.3 Comment est régi le cloud computing dans votre Pays ? Quelles mesure de sauvegarde / protection et quels standards sont obligatoires à cet effet ? Existe-t-il des exigences particulières relatives au stockage de données médicales sur le cloud ? Comment le partage de données est-il organisé ? Le partage fait-il l'objet de règles spécifiques ?

Voir la réponse à la question 2.2.

2.4 Existe-t-il des programmes gouvernementaux en vue de favoriser le data mining de données médicales ? Si oui, quels en sont les objectifs ? Des entités privées sont-elles autorisées à accéder à ces données ? Dans quelles circonstances / conditions ? Quelles sont les techniques / technologies utilisées ? A quelles fins ? Les personnes dont les données médicales sont utilisées en sont-ils informés ?

Il n'existe pas de tels programmes en Principauté.

2.5 Les entités privées sont-elles autorisées à extraire les données médicales qu'elles traitent ? Dans quelles circonstances / conditions ? Le Gouvernement a-t-il accès à ces données ?

La question paraît être sans objet en Principauté et, en tout état de cause, toute « extraction » ne pourrait être effectuée que dans le respect des dispositions de la loi n° 1.165 du 23 décembre 1993. Aussi, si le Gouvernement devait avoir connaissance de telles données, ce ne pourrait

être que dans le respect des règles susvisées. Cette « extraction » nécessiterait sans doute l'anonymisation de telles données.

2.6 Le Gouvernement et le secteur privé sont-ils autorisés à faire usage de méthode de profilage à partir de données médicales ? Si oui, dans quelles circonstances /conditions ? Le croisement et la mise en corrélation de données non médicales avec des données médicales (ou inversement) sont-ils autorisés ?

De telles méthodes ne sont possibles qu'à la condition d'être conformes aux dispositions de la loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives.

En principe, selon le premier alinéa de l'article 12 de cette loi, « *nul ne peut mettre en œuvre des traitements, automatisés ou non, faisant apparaître, directement ou indirectement, des opinions ou des appartenances politiques, raciales ou ethniques, religieuses, philosophiques ou syndicales, ou encore des données relatives à la santé, y compris les données génétiques, à la vie sexuelle, aux mœurs, aux mesures à caractère social* ».

Cette interdiction fait toutefois l'objet de dérogations prévues par les alinéas suivants dudit article. Ainsi, les dispositions de ce premier alinéa ne s'appliquent pas :

« *- lorsque la personne concernée a librement donné son consentement écrit et exprès, notamment dans le cadre de la loi n° 1.265 du 23 décembre 2002 relative à la protection des personnes dans la recherche biomédicale, sauf dans le cas où la loi prévoit que l'interdiction visée au premier alinéa ne peut être levée par le consentement de la personne concernée. Cette dernière peut, à tout moment, revenir sur son consentement et solliciter du responsable ou de l'utilisateur du traitement la destruction ou l'effacement des informations la concernant ;*

- lorsqu'un motif d'intérêt public le justifie, aux traitements [automatisés d'informations nominatives qui ont pour responsables des personnes morales de droit public, des autorités publiques, des organismes de droit privé investis d'une mission d'intérêt général ou des concessionnaires d'un service public et] *dont la mise en œuvre est décidée par les autorités ou organes compétents après avis motivé de la commission de contrôle des informations nominatives ;*

- lorsque le traitement concerne les membres d'une institution ecclésiale ou d'un groupement à caractère politique, religieux, philosophique, humanitaire ou syndical, dans le cadre de l'objet statutaire ou social de l'institution ou du groupement et pour les besoins de son fonctionnement, à condition que le traitement se rapporte aux seuls membres de cet organisme ou aux personnes entretenant avec lui des contacts réguliers liés à sa finalité et que les informations ne soient pas communiquées à des tiers sans le consentement des personnes concernées ;

- lorsque le traitement est nécessaire aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins, de médications ou de la gestion des services de santé et de prévoyance sociale, ou dans l'intérêt de la recherche et que le traitement de ces données est effectué par un praticien de la santé soumis au secret professionnel ou par une autre personne également soumise à une obligation de secret ;

- lorsque le traitement porte sur des informations manifestement rendues publiques par la personne concernée ;

- lorsque le traitement est nécessaire à la constatation, à l'exercice ou la défense d'un droit en justice ou répond à une obligation légale. »

En outre, l'article 10-2 de la loi n° 1.265 du 23 décembre 2002 impose que le traitement soit justifié :

« *- par le consentement de la ou des personnes concernées, ou ;*

- par le respect d'une obligation légale à laquelle est soumis le responsable du traitement ou son représentant, ou ;

- par un motif d'intérêt public, ou ;

- par l'exécution d'un contrat ou de mesures pré-contractuelles avec la personne concernée, ou ;

- par la réalisation d'un intérêt légitime poursuivi par le responsable du traitement ou son représentant ou par le destinataire, à la condition de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée ».

Dans ce cadre et en tout état de cause, l'article 10-1 de la loi susmentionnée dispose que les informations nominatives doivent notamment être :

« *- collectées pour une finalité déterminée, explicite et légitime, et ne pas être traitées ultérieurement de manière incompatible avec cette finalité ;*

- adéquates, pertinentes et non excessives au regard de la finalité pour laquelle elles sont collectées et pour laquelle elles sont traitées ultérieurement ».

3.2 Existe-t-il un cadre juridique spécifique à la radio-identification (radio frequency identification, soit l'identification via puce électronique (utilisée aussi pour des cartes de transport par exemple), éventuellement sous-cutanée) et au transfert de données personnelles par technologies sans fil ? Dans la négative, comment le droit commun de la protection des données peut-il être appliqué pour couvrir ces domaines ? Indiquer les textes, jurisprudence, normes ou recommandations pertinents en la matière.

Même réponse que précédemment, il n'existe pas de textes spécifiques, ce qui conduit à considérer que le droit commun est applicable.

A cet égard, la CCIN a précisé avoir été consultée pour la mise en place de tels dispositifs, notamment dans le domaine du transport. Dans ces cas, la Commission s'est intéressée aux mesures de sécurité mises en place par les responsables de traitement afin de respecter les dispositions des articles 17 et suivants de la loi n° 1.165 du 23 décembre 1993.

3.3 Comment est utilisée la radio-identification dans les hôpitaux – établissements de santé – cliniques en tant qu'instrument de gestion des ressources humaines. Est-elle utilisée aux fins de soins pour les patients ? Quels types de système de base de données ou de système de sécurité sont mis en œuvre en complément de l'utilisation de la radio-identification ? Comment sont traitées les questions qui ont trait au consentement, à l'accès ou au partage au vu du fait que la radio-diffusion pourrait être utilisée sans que le patient en ait connaissance ?

En pratique, il peut être fait usage de procédés d'authentification forte via carte à puce et RFID pour une authentification aux applications.

Les professionnels de santé qui ont la charge des patients disposent d'un accès au dossier médical via ces procédés d'authentification.

En cas d'accès pour des circonstances exceptionnelles, dit accès « bris de glace », ces derniers sont bien tracés et les patients peuvent avoir accès sur demande à ces consultations réalisées suite à de telles circonstances.

3.4 Les hôpitaux – établissements de santé – cliniques utilisent-ils d'autres techniques de surveillance (permettant de tracer) sans fil en complément de la radio-identification ? Lesquelles ? Doivent-ils respecter des mesures / obligations spécifiques ? Si oui, lesquelles ?

Certains dispositifs médicaux utilisés par les établissements de santé sont connectés à des réseaux sans fil cryptés et non diffusés.

4.2 Existe-t-il un cadre juridique spécifique aux applications et aux applications de smartphones ? Dans la négative, comment le droit commun de la protection des données peut-il être appliqué pour couvrir ces domaines ? Indiquer les textes, jurisprudence, normes ou recommandations pertinents en la matière.

Même réponse que précédemment s'agissant des dispositions spécifiques et de l'application du droit commun des données personnelles et de la protection des consommateurs.

La CCIN a indiqué ne pas avoir été saisie sur ce sujet.

4.3 La collecte de données médicales et la mise en place de services médicaux via applications / applications de smartphones est-elle autorisée ? Si oui, quelles sont les personnes / entités autorisées à y avoir recours ? Existe-t-il des règles / mesures / obligations spécifiques à cet effet ?

Certains établissements de santé travaillent sur la mise en place d'un accès « smartphone » à la dictée de compte-rendu patient, ainsi qu'à l'affichage d'agenda de ressources ou des patients. Ces applications seraient diffusées par un outil de mobile management maîtrisé par l'établissement lui-même. Il serait fait usage d'un procédé d'identification forte.

4.4 Les hôpitaux – établissements de santé – cliniques – laboratoires ont-il recours à des applications aux fins de rassembler des données médicales ? L'utilisation d'application à des fins de traitements de données médicales est-elle justifiée par un traitement médical ? Existe-t-il des règles / mesures / obligations spécifiques pour les institutions qui collectent de telles données à partir de ces applications ? Des données « médico-administratives » sont-elles utilisées à des fins de gestion des ressources humaines ?

Certains établissements de santé mettent à disposition des professionnels un dossier patient informatisé comprenant des données médicales et médico-administratives. Il est fait application des dispositions de la loi n° 1.165 du 23 décembre 1993 précitée.

4.5 Existe-t-il des exigences particulières tenant à la protection de la vie privée dans le développement des applications ou des systèmes de surveillance à des fins médicales ? Si oui, quels sont les standards ?

Il est fait application des dispositions de la loi n° 1.165 du 23 décembre 1993 susmentionnée, sous les préconisations, recommandations et avis de la Commission de Contrôle des Informations Nominatives.

4.6 Le système repose-t-il sur l'adhésion de la personne concernée ? La collecte doit-elle être en lien avec un diagnostic médical ? Comment cela pourrait-il être appliqué en matière sportive ou pour les données liées au quotidien ?

La collecte des informations est en lien avec un diagnostic médical ou à des fins de recherches, conformément aux dispositions de la loi n° 1.165 du 23 décembre 1993. Le consentement du patient est alors pris en compte en tant que préalable et la déclaration est effectuée auprès de la Commission de Contrôle des Informations Nominatives.

5**.1 On entend par dispositif médical : tout instrument, appareil, équipement, matière ou autre article, utilisé seul ou en association, y compris le logiciel nécessaire pour le bon fonctionnement de celui-ci, destiné par le fabricant à être utilisé chez l'homme à des fins :**

- **de diagnostic, de prévention, de contrôle, de traitement ou d'atténuation d'une maladie,**
- **de diagnostic, de contrôle, de traitement, d'atténuation ou de compensation d'une blessure ou d'un handicap,**
- **d'étude ou de remplacement ou modification de l'anatomie ou d'un processus physiologique,**
- **de maîtrise de la conception,**

et dont l'action principale voulue dans ou sur le corps humain n'est pas obtenue par des moyens pharmacologiques ou immunologiques ni par métabolisme, mais dont la fonction peut être assistée par de tels moyens.

5.2 Existe-t-il un cadre juridique spécifique applicable aux dispositifs médicaux ? Dans la négative, comment le droit commun de la protection des données peut-il être appliqué pour couvrir ces domaines ? Indiquer les textes, jurisprudence, normes ou recommandations pertinents en la matière.

Il s'agit de la loi n° 1.267 du 23 décembre 2002 relative aux dispositifs médicaux, dont la définition reprend celle susvisée. Pour autant, celle-ci ne contient pas de dispositions spécifiques à la protection des informations nominatives. Aussi le droit applicable demeure-t-il la loi n° 1.165 du 23 décembre 1993.

5.3 Le concept de dispositif médical, selon l'acception retenue par votre Pays, englobe-t-il les services et vêtements en lien avec le domaine de l'e-santé ou de la « santé mobile » (mhealth) ? Quelles sont les exigences ? Par exemple, les dispositifs médicaux ne devraient-ils pas passer par un processus de certification avant utilisation ?

La réponse à cette question ne peut être formulée de manière tranchée, tout est question de l'interprétation qui pourrait être donnée de la législation en vigueur en fonction de la nature et de la finalité précise de tels objets. Aussi, à défaut de disposer de définitions juridiques précises de ces termes ou d'un rattachement en ce sens à la notion de dispositifs médicaux ou d'accessoires d'un dispositif médical, il ne peut être question que de casuistique.

5.4 Le concept de dispositif médical, selon l'acception retenue par votre Pays, englobe-t-il les applications ? Existe-t-il des règles applicables aux dispositifs médicaux qui utilisent de telles applications ? Même question s'agissant d'applications qui tracent des données non-médicales qui peuvent conduire à l'obtention d'informations sur la santé. Si oui, quels sont les types de données concernés ?

Réponse identique au 5.3.

5.5 Existe-t-il des exigences particulières tenant à la protection de la vie privée dans le développement des dispositifs médicaux ou dispositifs médicaux portables (type montres par exemple) ? Si oui quels sont les standards applicables ?

A priori sans objet.

5.6 Le système repose-t-il sur l'adhésion de la personne concernée ? La collecte doit-elle être en lien avec un diagnostic médical ? Comment cela pourrait-il être appliqué en matière sportive ou pour les données liées au quotidien ?

A priori sans objet.

6.2 Existe-t-il un cadre juridique spécifique applicable aux objets disposant d'une connexion à Internet ou objets connectés ? Dans la négative, comment le droit commun de la protection des données peut-il être appliqué pour couvrir ces domaines ? Indiquer les textes, jurisprudence, normes ou recommandations pertinents en la matière.

Il n'existe pas de cadre juridique spécifique applicable aux objets connectés, lesquels sont donc soumis aux règles du droit commun, notamment à celles fixées par les lois n° 1.165 du 23 décembre 1993 et n° 1.383 du 2 août 2011.

La CCIN a indiqué ne pas avoir été saisie de cette problématique.

6.3 Quels sont les standards de sécurité qui doivent être employés par ces dispositifs quand ils collectent des données personnelles ?

Voir la réponse à la question 6.2.

6.4 Les dispositifs non médicaux sont-ils autorisés à collecter des données médicales, comme la fréquence cardiaque ? Sont-ils autorisés à croiser des données non-médicales avec des données médicales ?

Voir la réponse à la question 6.2.

6.5 Existe-t-il des exigences particulières tenant à la protection de la vie privée dans le développement des objets connectés ? Si oui quels sont les standards applicables ?

Voir la réponse à la question 6.2.

7.2 Existe-t-il un cadre juridique spécifique applicable aux traitements médicaux en ligne (consultations médicales en ligne ?) ainsi que les systèmes de rendez-vous médicaux en ligne ? Dans la négative, comment le droit commun de la protection des données peut-il être appliqué pour couvrir ces domaines ? Indiquer les textes, jurisprudence, normes ou recommandations pertinents en la matière.

Il n'existe pas de cadre juridique spécifique applicable aux consultations médicales en ligne.

Il pourrait cependant résulter du deuxième alinéa de l'article 52 du Code de déontologie médicale, selon lequel « *l'avis ou le conseil dispensé à un patient par téléphone ou par correspondance ne peut donner lieu à aucun honoraire* », que de telles consultations devraient se limiter à un avis ou conseil et ne pourraient donner lieu à aucun honoraire.

En d'autres termes, cette disposition pourrait servir de fondement à une interdiction de toute consultation en ligne ayant pour objet de poser un diagnostic, notamment si l'on considère qu'un diagnostic ne saurait être posé avec suffisamment de certitude sans un examen physique du patient.

7.3 Les traitements médicaux (ou les consultations médicales) en ligne sont-ils autorisés ? Si oui, comment les services médicaux devraient-ils être fournis ? Doivent-ils suivre les mêmes obligations / règles / contraintes que les consultations physiques ?

Voir la réponse à la question 7.2.

7.4 Comment devraient être traitées les données collectées à l'occasion d'une consultation médicale en ligne ? Existe-t-il des règles / obligations spécifiques ? Lesquelles ?

Voir la réponse à la question 7.2.

NORWAY / NORVÈGE

QUESTIONNAIRE

The questionnaire should ideally be completed by data protection authorities, health policy authorities, professional or patient associations as well as healthcare providers: you are invited to share it as widely as possible.

Please send your replies to dataprotection@coe.int no later than 15 December 2014.

1. Mobile Health (mHealth) and Electronic Health Records (EHR)

1.1. Data Protection Issues:

This is perhaps the biggest topic sitting at the intersection of technology and data protection. Mobile health (mHealth) and Electronic Health Records (EHR) are increasingly used in healthcare systems and provisions – it is a trend that needs to be examined.

Related to the EHR, these records are more accurate, cost-effective (in terms of storage) than paper-based notes. The concept of patient controlled/accessed EHR has been implemented in varying degrees in different countries.

Furthermore, some non-medical record can still contain health information about users and it should be considered if such records ought to be treated in a similar way to EHR.

Also, should 'medical data' as defined in Recommendation N° (97) 5 on the protection of medical data cover physical tracking data, such as pedometers or fitness data and data that can lead to medical information about an individual ?

1.2. Questions: if EHR exist in your country, is your legal framework providing for a regulation of such records? If mHealth exists in your country, is your legal framework providing for a specific regulation? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	Personal Health Data Filing Systems Act (2001) http://lovdata.no/lov/2001-05-18-24 Personal Data Act http://lovdata.no/lov/2000-04-14-31 Act relating to health personnel etc http://lovdata.no/lov/1999-07-02-64
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
EHR and Medical data:	What can be considered medical data in your country? Is it solely the data relating to a person's health (state, diagnosis, prognosis, medical treatment, etc.)? Is non-medical data that leads to medical information treated the same way as medical data (for instance in terms of confidentiality requirements)? Is the EHR solely constituted of data collected in a medical context or can the individual also himself or herself add information regarding his or her health?

	Medical data (health-related data) are data related to a person's health, that are collected/registered by health professionals giving the person health care as part of a health care service or collected as a part of the administration of health care services. Health related data are covered by the provisions on duty of confidentiality in the Health Personnel Act. Data collected by a person for his or her own use are not considered to be health-related data. If health information is processed by other professionals that are not health care providers and who are not bound by the duty of confidentiality provisions of the Health Personnel Act, the Personal Data Act provisions concerning sensitive personal data will apply. Act is enforced by the Data Inspectorate.
Sharing of data and Access:	Who is granted access to the EHR and how is the sharing of information (with other health care providers?) regulated? Where information is shared with pharmacists, is there a strict purpose limitation in place? How has the definition of the responsibility over the medical data been regulated?
	Only health personnel who need the information to be able to provide health care to the person are allowed to access his/her health records. Also only persons working in the organization that is responsible for the patient records(for instance the hospital) can access a patient record. A pharmacist will only have the prescription and may not access the person's health record. Organisations in the health service/health administration must give notification to the Data Inspectorate of their use of personal health data pursuant to the Personal Health Data Filing Systems Act. This applies, inter alia, in case of: • use of medical records. • some research projects • local, regional and central health data filing systems regulated by the Personal Health Data Filing Systems Act. All health data filing systems, including electronic health records must have a designated Data Controller. The Data Controller is responsible for purpose limitation and for information security. Information security includes ensuring confidentiality, integrity and quality of the information as well as restricting access to the health records so that only persons who need access to a person's health information may access it.
Data quality:	Are the principles of legitimacy, fairness and minimisation applied to medical data? How are records kept accurate? How long is the data kept for, is the specific storage period defined for the EHR?
	According to the Health Personnel Act health personnel have a duty to keep health records for each individual patient to document their work. The law states that records shall only contain relevant and necessary information about the patient and the health care, as well as the information that is required in order to comply with the notification requirements or the duty of disclosure laid down in or pursuant to law. What is deemed relevant and necessary is further specified in the Health Record Regulation. The health professional giving health care to the patient is responsible for keeping the record accurate.

	There is no specific storage period defined for EHR. According to the Health Record Regulation the health records must be kept until it must be supposed that they will no longer be of use, based on the character of the health care that has been provided. When they are no longer needed, they must be deleted. However, the health record archives of public health care providers cannot be deleted. They are to be deposited in an archive subject to public archive provisions. Public health records may be deposited when 10 years have passed since the last entry.
Data integrity:	Are any specific methods used to ensure the integrity of the data? How are patients identified in the EHR? In the context of research, are anonymisation methods used and what safeguards exist for re-identification?
	Only health personnel providing health care to the patient may enter health-related data into the health record. Accessing the health records of a patient is prohibited for anyone who does not need to access them in order to treat the patient or for administrative purposes, unless access is authorized by law. Patients are identified by a national identity number. Non-anonymous health related data may be used in health research only if this has been pre-approved by a regional research ethics committee. As a main rule the explicit and informed consent of the patients is required in addition. Dispensation from the consent requirement may be given if provided for by law. If a research project is not considered to be "health research", the project will need a licence from the Data Inspectorate in addition to consent from the persons in order to process health information.
Data security:	Where are the records stored? Is there a centralised database of EHR? What security technology is being used?
	As long as data security is ensured, this is up to the Data Controller. Norway has one centralized electronic health record, called the National Core Health Record. This record only contains certain specific ("core") elements concerning each individual, and is to be used in emergency situations where access to the full medical records of a patient is impossible.
Rights of the person/patient concerned:	How can the right of access be exercised? How can the data be corrected? Can the person enter information in his or her own EHR? What are the legal remedies available?
	Every patient may ask for a copy of his/her health record, except in rare cases. They also have a right to see the log that shows who has accessed his/her electronic health record. It will be possible for the patients to have electronic access to view their information in the National Core Health Information Record. They will also be able to enter some personal information in addition to the predefined information elements. Patients may not access or enter information into the electronic health records that are kept by the health professionals/health institutions. A patient may demand that information in his/her health record is corrected or deleted. Procedures for how health records may be corrected/deleted and who can do it are specified in the Health Personnel Act sections 42 and 43.

	A patient may file a complaint with the County Governor if the patient thinks that his/her rights regarding the health records are not fulfilled.
Consent:	Is the system based on an opt-in approach? Is the principle of granular consent applied (with the possibility of preventing access to certain data?)? If yes, in which situations?
	Health personnel are obliged to keep health records, and the patient must accept that this is part of the health care. The patient may decide that access to his/her health record shall be restricted, or that access to certain information shall be restricted, and who shall be allowed/not allowed access. Patient records may be transferred or released to other health personnel if this is necessary in order to provide health care in a responsible manner. The patient may object thereto. Patients have a right to object to being included in the National Core Health Information Record, or to restrict access to certain information in this record.
Withdrawal:	Are patients able to withdraw the consent given to EHR schemes? If yes, what is the relevant procedure to withdraw such consent? What are the consequences?
	Patients may withdraw their consent to being registered in the National Core Health Information Record at any time. If they do, their information shall be deleted. Other health records are not based on the patient's consent as this is a duty for the health personnel.
Outsourcing processing of data:	Is outsourcing common? Under what circumstances? Where is the data outsourced to? What sort of safeguards are in place?

2. Cloud Computing, Data Mining and Profiling from both Medical Records (including EHR) and Data not specifically related to medical records.

2.1. Data Protection Issues:

Cloud computing has brought a new dimension to the way data is stored, accessed and processed. Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS), Network as a service (NaaS) are all used by services and organisations that deal with both medical data and non-medical data.

With the development of more advanced and efficient data-mining and data-querying Medical techniques (e.g NoSQL, MapReduce, Hadoop) in conjunction with increased processing power and data storage, mining data has never been more informative, easier, and cost-effective.

Healthcare is a natural sector in which to apply new technologies and methodologies, with particular impacts in epidemiology, public health, health services research, etc.

Data that can lead to the identification of a particular individual and his/her health situation is not limited to medical data *per se,* present on Electronic Health Records, but also to unsuspicious type of information.

There is a growing concern that these schemes may be implemented in manner which does not always respect the patients' confidentiality and basic rights, and in a broader context, the use of this of information may prejudice the individuals concerned.

The ability to track and monitor patients and resources enables a more efficient provision of care but may have an impact on the right to privacy of the individual concerned.

2.2. Questions: Is your legal framework providing for a regulation of Cloud Computing, Data Mining and Profiling? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Cloud computing:	How is cloud computing regulated in your country? Which security safeguards and standards are mandatory? Are there specific requirements in order to store medical data in the cloud? How is data shared and is the sharing regulated?
Government:	Do governmental programmes exist to allow for increased data-mining of medical records? If yes, what are the purposes of this data mining? Are private entities allowed to access the data? Under what circumstances? What sort of techniques and technologies are being used? To what end? Are data subjects informed of this type of data-mining?
Private sector:	Are private entities allowed to mine medical data which they process? Under what circumstances? Can the government have access to this data?
Profiling:	Are the government and the private sector allowed to employ profiling methods on medical data? If yes, under what circumstances? Is it allowed to cross and correlate non-medical data with medical data?

3. RFID and wireless communication technologies

3.1. Data Protection Issues:

It is common for medical devices, such as patients' tags, to possess RFID technologies in order to facilitate the transmission of the patients' data.

It can also be related to the data-mining operations previously mentioned as it is another category of information that can be used to discern meaningful patterns.

Transmission of data through radio-frequency is not limited to medical devices. Almost any smartphone uses some technology enabling to collect, and share, the user's data. For instance, via WI-FI it is possible to identify users' locations and therefore infer some of their behaviour, which in some cases can relate to health information.

3.2. Questions: Is your legal framework providing for a regulation of RFID technologies and the transfer of personal data through wireless technologies? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
RFID:	How is RFID used in hospital/clinics for (a) resource management, (b) patient care? What types of database systems (and security) are implemented in conjunction with RFID use? How are issues of access, sharing, consent etc. managed considering that RFID may be used without the patients' knowledge.
Wireless tracking technologies:	Are hospitals/clinics employing other wireless tracking technologies besides RFID? Which ones? Do they have to follow specific security requirements? Which ones?

4. Applications (Mobile)

4.1. Data Protection Issues:

Information society is increasingly relying on the use of "apps" (application), most of them mobile. These apps are commonly designed to gather personal data, and in practice often process medical data.
Technologies such as multi-touch touchscreen, accelerometers or gyroscopes, ambient light sensors, GPS and cameras, and devices featuring fingerprint and biometric sensors also involve the collection of medical data.

A mobile phone application can monitor accurately physiological data, such as heartbeats, sleep patterns, fitness information.

4.2. Questions: Is your legal framework providing for a regulation of Apps and Mobile Apps? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Apps:	Is it allowed to use apps and mobile apps to deploy medical services and collect medical data? If yes, which type of individual/organisation can develop and employ these apps? Are there specific security requirements for these types of apps?

Institutions:	Do hospitals/clinics/labs employ apps to gather medical data? Is there a need for a medical treatment to permit the use of an app to process the medical data? Are there specific security requirements for the institutions collecting these data from the apps? Are medico-administrative data used by hospitals/clinics for management purposes?
Tracking technologies:	Do hospitals/clinics/labs employ non-medical apps and devices to track and collect data from their patients? What type of data is collected? For what purpose? Is the data identifiable? Is the data combined with medical data?
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical apps and tracking apps? If yes, what are the standards?
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical diagnostic? How would this be applied to fitness and daily-basis data?

5. Medical Devices and Wearable Devices

5.1. Data Protection Issues:

A medical device can be defined as: 'any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application. Such a device should be intended by the manufacturer for one of a number of defined purposes, one of which is, diagnosis, prevention, monitoring, treatment or alleviation of disease' (Directive 93/42/EEC Article 1:2)

Some eHealth and mHealth devices and apps do not fall in this definition of medical devices, as can also be the case of a software working in combination with a physical device, for instance a smartphone.

5.2. Questions: Is your legal framework providing for a regulation of Medical Devices? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
eHealth and mHealth:	Does the concept of Medical device in your country encompass services and apparels in the realm of eHealth and mHealth? What are the requirements? Should, for instance, the medical device be certified before it can be used?

Apps:	Does the concept of medical devices encompass apps? If yes, is there any regulation applicable to apps that perform medical services? Is there any regulation applicable on apps that track non-medical data that can lead to health information? If yes, what type of data?
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical and/or wearable devices? If yes, what are the standards?
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical treatment? How would this be applied to fitness and daily-basis data?

6. Internet of Things

6.1. Data Protection Issues:

Internet of things relates to common, ordinary devices that are now, and increasingly, connected to the Internet, such as cars, fridges, ovens, microwaves, etc. All of these devices can provide data that can lead to reveal information concerning one's health. A fridge can easily inform on the type of food stored and thus the diet of an individual. One of the biggest challenges of the Internet of Things is to guarantee the right to privacy and data protection in a world where every device collects, processes, analyses and transmits the data, commonly via wireless technologies.

In the realm of medical data, the issue mainly arises when crossing seemly unrelated data that can lead to health information about an individual.

6.2. Questions: Is your legal framework providing for a regulation of the Internet of Things? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Security:	What are the security standards that need to be employed by these devices when collecting personal data?
Non-medical devices:	Are non-medical devices allowed to collect medical data, such as heart frequency? Are they allowed to cross medical data with non-medical data?
Privacy by Design:	Is there any requirement to implement privacy by design in the development of connected devices? If yes, what are the standards?

7. Electronic Doctor (online Doctor) and on-line appointments

7.1. Data Protection Issues: The Doctor listens, talks and assesses the patient online, via a website, app, canal, sometimes including video-conference. Medical data is collected and processed, what are the security requirements and standards followed? Other websites provide for on-line appointments with doctors, which can also involve the processing of medical data.

7.2. Questions: Is your legal framework providing for a regulation of online Medical Treatment and is the on-line appointment system covered by such a framework? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Medical treatment:	Is it allowed to perform medical treatment via online services? If yes, how should the medical services be provided? Does it have to follow the same requirements of a regular physically-present medical treatment?
Medical data:	How should the data collected via a medical treatment performed online be processed? Are there specific requirements? Which ones?

Other comments and technologies
Should you wish to describe any technology, feature or trend that has not been covered by the questionnaire, please feel free to use the space provided below. Where relevant, also indicate recent legislation changes, guidelines and/or case law.

POLAND / POLOGNE

QUESTIONNAIRE

The questionnaire should ideally be completed by data protection authorities, health policy authorities, professional or patient associations as well as healthcare providers: you are invited to share it as widely as possible.

Please send your replies to dataprotection@coe.int no later than 15 December 2014.

1. Mobile Health (mHealth) and Electronic Health Records (EHR)

1.1. Data Protection Issues:

This is perhaps the biggest topic sitting at the intersection of technology and data protection. Mobile health (mHealth) and Electronic Health Records (EHR) are increasingly used in healthcare systems and provisions – it is a trend that needs to be examined.

Related to the EHR, these records are more accurate, cost-effective (in terms of storage) than paper-based notes. The concept of patient controlled/accessed EHR has been implemented in varying degrees in different countries.

Furthermore, some non-medical record can still contain health information about users and it should be considered if such records ought to be treated in a similar way to EHR.

Also, should 'medical data' as defined in Recommendation N° (97) 5 on the protection of medical data cover physical tracking data, such as pedometers or fitness data and data that can lead to medical information about an individual ?

1.2. Questions: if EHR exist in your country, is your legal framework providing for a regulation of such records? If mHealth exists in your country, is your legal framework providing for a specific regulation? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	**Project P1** **Currently, the works on the so called Project P1 are conducted in Poland. Project P1 is an undertaking realised in the public healthcare system in Poland for the purpose of improving the quality of healthcare services. Project P1 is realised by the Centre of Health Information Systems, a unit subordinate to the Ministry of Health, and is financed from EU funds. Within the framework of this project the following electronic services will be available: the Internet Patient Account, electronic prescription, referral, order, and eHealth Information Portal will be provided. The services will be available to patients, doctors and pharmacists.** **ZIP** **The Integrated Patient Guide (ZIP) is kept by the National Health Fund. ZIP is a country-wide service making available to registered users historical data on their treatment and its financing, collected by the National Health Fund since 2008. Access to the data can be obtained on the Internet with the use of a tool equipped with a search engine. Access to ZIP is possible for patients. The data are physically stored in the National Health Fund.**

eWUS

The eWUS system (Electronic Verification of Beneficiaries' Eligibility) is a system enabling immediate confirmation of the patient's right to healthcare services financed from public funds. Access is possible for medical institutions. Access can be also obtained on the Internet with the use of a tool equipped with a search engine. The data are physically stored in the National Health Fund.

The Act of 28 April 2011 on the healthcare information system (Journal of Laws of 2011.113.657), which specifies the organisation and operation of the healthcare information system, called the "information system". In the latter system, the data necessary to conduct the state health policy, increase quality and availability of healthcare and finance healthcare tasks are processed. The Act defines the notion of "electronic medical documentation"[electronic health record] (Art. 2 point 6 a and b) as:

a) **an electronic document enabling the service user to obtain a specific type of healthcare service, in case of service provider being a healthcare provider referred to in Art. 5 point 41 letter d of the Act of 27 August 2004 on healthcare services financed from public resources (Journal of Laws of 2008 No. 164, item 1027, with later amendments), a publicly available pharmacy or pharmaceutical point,**

b) **medical documentation, referred to in the Act of 6 November 2008 on Patients' Rights and the Commissioner for Patients' Rights (Journal of Laws of 2009 No. 52, item 417 and No. 76, item 641, of 2010 No. 96, item 620), produced in electronic form, containing data on provided, being provided and planned healthcare services, including electronic document enabling the service user to obtain a specific type of healthcare service, in case of service provider other than the one mentioned in letter a.**

The Act on Patients' Rights and the Commissioner for Patients' Rights indicates that the entity providing healthcare services shall be obliged to keep, store and disclose medical documentation in a way specified in this chapter and ensure the protection of data contained in this documentation. Medical documentation shall be kept in electronic form (Art. 24 para. 1 and 1a). In June 2014 the Act on the healthcare information system was amended in terms of moving the deadline of the obligation to keep medical documentation (EDM) in electronic form for 1 August 2017.

Pursuant to Art. 11 of the Act on healthcare services financed from public resources it is the service providers who shall be obliged to keep electronic medical documentation.

As regards notification obligation, pursuant to Art. 43 para. 1 point 5 of the Act on Personal Data Protection the obligation to register data filing systems shall not apply inter alia to the controllers of data which refer to the persons availing themselves of their health care services. In connection with this the data filing system kept by entities providing medical services and containing patients' data are not notified to the Polish DPA. However, the notification obligation applies to data controllers who do not provide healthcare services by themselves, but process the data of persons using medical services of other entities.

Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
EHR and Medical data:	What can be considered medical data in your country? Is it solely the data relating to a person's health (state, diagnosis, prognosis, medical treatment, etc.)? Is non-medical data that leads to medical information treated the same way as medical data (for instance in terms of confidentiality requirements)? Is the EHR solely constituted of data collected in a medical context or can the individual also himself or herself add information regarding his or her health?
	Art. 2 point 7 on the healthcare information system defines individual medical data – personal data and other data of natural persons concerning the rights to provided, being provided and planned healthcare services, health condition and other data processed in connection with planned, being provided and provided healthcare services as well as preventive medicine and execution of health programmes. **Art. 24 of the Act on patients' rights and protection of patients' rights sets forth that the entity providing healthcare services shall be obliged to keep, store and disclose medical documentation in a way specified in this chapter and ensure the protection of personal data contained in this documentation. Medical documentation shall be kept in electronic form.** **Art. 27 para. 1 of the Act on Personal Data Protection includes in the catalogue of sensitive data "health data" and makes the processing of health data subject to specific, stricter requirements (as a rule the processing of such data is prohibited, and allowed only in cases indicated in para. 2 of the mentioned Article).** **In the light of the definition contained in Art. 2 para. 1 point 1 of the Act of 15 April 2011 on medical activity (Journal of Laws No. 112, item 654, with later amendments) medical documentation shall mean the documentation referred to in the provisions of the Act of 6 November 2008 on patients' rights and the Commissioner for Patients' Rights (unified text: Journal of Laws of 2012, item 159 with later amendments).** **The general principle is to keep patient related information confidential and not to disclose such information to third persons. Such obligation is imposed on persons practicing medical professions by Art. 13 of the Act of 6 November on patients' rights and the Commissioner for Patients' Rights (unified text: Journal of Laws of 2012, item 159; hereinafter referred to as APRCPR). Such regulation is also included in Art. 40 of the Act of 5 December 1996 on doctor's profession and dentist's profession (unified text: Journal of Laws of 2011 no. 277 item 1634; hereinafter referred to as ADPDP) with reference to doctors and dentists.** **Patient related information, in particular information on patient's health, which was obtained by healthcare professionals in connection with practicing of medical profession, is subject to secrecy. Thus both information disclosed in connection with provision of health service directly related with patient's personal, professional or public life as well as data identified by persons practicing medical profession in the course of professional activities, e.g. results of conducted tests, diagnosis, etc., are confidential. The confidentiality obligation is applicable regardless of the fact, whether the doctor obtained specific information directly from the**

	patient or from third person, or even regardless of the fact of obtaining specific information against patient's will. **Commonly known facts and circumstances are, however, not protected by secrecy, even if a doctor or other person practicing a medical profession, who had not known about such facts or circumstances, learnt about them in connection with practicing of their profession.**
Sharing of data and Access:	Who is granted access to the EHR and how is the sharing of information (with other health care providers?) regulated? Where information is shared with pharmacists, is there a strict purpose limitation in place? How has the definition of the responsibility over the medical data been regulated?
	The patient's right of access to medical documentation concerning his/her health and health services provided to him/her is strictly connected with the patient's right to information on his/her health, diagnosis, diagnostic and treatment methods, consequences of their use or failure to use, results of treatment, prognosis. The patient has also the right to the protection of data contained in medical documentation (Art. 23 of the Act on patients' rights and the Commissioner for Patients' Rights). **Doctors, nurses and midwifes have the right to obtain and process the data contained in medical documentation (Art. 24 para. 2 of the above Act).** **Pursuant to Art. 26 of the above Act the entity providing healthcare services makes available medical documentation to a patient or his/her statutory representative or a person authorized by the patient. After the patient's death, the person authorised by the patient during his/her lifetime has the right to consult medical documentation.** **The entity providing healthcare services discloses medical documentation also to:** **1) entities providing healthcare services, if the documentation is necessary to ensure continuity of provision of healthcare services;** **2) public authorities, the National Health Fund, bodies of self-governments of medical professions as well as national and voivodeship consultants, in the scope necessary for those entities to realize their tasks, in particular control and supervision;** **2a) entities referred to in Art. 119 para. 1 and 2 of the Act of 15 April 2011 on medical activity, in the scope necessary to conduct inspections ordered by the Minister of Health;** **3) the Minister of Health, courts, including disciplinary courts, public prosecutors, court-appointed doctors, and screeners for professional liability, in connection with conducted proceedings;** **4) bodies and institutions authorised under separate acts, if the examination was conducted upon their request;** **5) pension authorities and disability assessment boards, in connection with proceedings conducted by them;** **6) entities keeping medical services registers, in the scope necessary to keep registers;**

	7) insurance companies, with the patient's consent; **8) a doctor, nurse or midwife, in connection with carrying out the procedure of assessment of the entity providing healthcare services based on the provisions on healthcare accreditation, in the scope necessary to carry out such procedure;** **9) the voivodeship committee adjudicating on medical events referred to in Art. 67e para. 1, in the scope of the conducted proceedings;** **10) heirs in the scope of conducted proceedings before the voivodeship committee adjudicating on medical events, referred to in Art. 67e para. 1;** **11) persons carrying out inspection activities on the grounds of Art. 39 para. 1 of the act of 28 April 2011 on healthcare information system (Journal of Laws No. 113, item 657 and No. 174, item 1039), in the scope necessary to conduct the above activities.** **Medical documentation may be disclosed also to a university or research institute to be used for medical purposes, without disclosing the name, etc. Documentation is disclosed in electronic form by:** **1. providing an IT data carrier containing a recorded copy of documentation,** **2. electronic transmission of documentation,** **3. providing paper print-outs upon request of authorised entities or authorities.** **If documentation in electronic form is disclosed, its integrity and personal data protection must be ensured. In case of disclosure of documentation kept electronically in the form of paper print-outs, the person authorised by the entity confirms their conformity with documentation in electronic form and marks it with his/her designation. Printed documentation shall enable identification of persons providing healthcare services.** **Art. 6 of the Act on healthcare information system introduces an ICT system – Platform for Sharing Online Services and Resources of Digital Medical Records, which allows in particular for: 1) communication of Medical Information System (MIS) with medical records in order to obtain the data processed in those records; 2) making updates of data in medical records; 3) integration of medical records; 4) disclosure of data from medical records, in the scope of granted authorizations, to service providers and payers.** **The controller of the system of the Platform for Sharing Online Services and Resources of Digital Medical Records is the unit subordinate to the Minister of Health, competent in healthcare IT systems (Centre of Health Information Systems).** **The above entity is also the controller of the system of Electronic Platform for Collection, Analysis and Sharing of Digital Medical Records on Medical Events (Art. 7 of the above Act). It is an ICT system enabling inter alia transferring by service providers to MIS information on provided, being**

	provided and planned healthcare services as well as sharing between service providers of data contained in electronic medical documentation, if it is necessary for ensuring continuity of treatment, as well as sharing of electronic documents between service providers in order to carry out diagnostics, to ensure continuity of treatment and to supply medicinal products or medical devices to the service users. **Pursuant to Art. 11 of the Act on healthcare services funded from public resources, electronic medical documentation shall be kept by service providers. The service provider with the agency of the Medical Information System[26] may obtain access to data, including personal data and individual medical data, contained in the service user's electronic medical documentation, stored in the ICT system of another service provider, if it is necessary to ensure continuity of treatment or conducted diagnostic procedure. The service provider includes in the Medical Information System the data enabling the download of the data contained in the electronic medical documentation by another service provider or the download of electronic documents necessary to carry out diagnostics, to ensure continuity of treatment and to supply medicinal products or medical devices to the service users.** **Access to the data processed in MIS depends on authorisations granted to the system user based on the Act or legal provisions on personal data as well as individual medical data. Access to the data under the conditions and in the scope specified in the provisions of the above indicated Act is granted to the service user[27], payers, voivode, medical professionals and service providers (in the scope of the tasks realised by them and the rights conferred to them, the data are disclosed, including personal data and individual medical data of service users), entities keeping medical records, territorial self-government units (in the scope of the tasks realised by them, resulting from the provisions regulating the tasks of the territorial self-government, in the scope of public health).**
Data quality:	Are the principles of legitimacy, fairness and minimisation applied to medical data? How are records kept accurate? How long is the data kept for, is the specific storage period defined for the EHR?
	For the purpose of exercise of the patient's right of access to medical documentation concerning his/her health condition and medical services provided to him/her the entity providing such services shall be obliged to keep and store medical documentation. **Medical documentation may be kept in two ways: in written or in electronic form. Keeping medical documentation in electronic form allows the healthcare services providers to quickly enter and search for data.** **In the light of the Regulation on the types and scope of medical documentation and the way of its processing, the basic terms of keeping medical documentation in electronic form for healthcare entities and professional practices are as follows:**

[26] MIS is an ICT system used for the processing of data concerning provided, being provided and planned healthcare services disclosed by the service providers' ICT systems.

[27] The service user has the right of access to data, including personal data and individual medical data concerning him/her, in the scope necessary to exercise the rights specified in the Act, i.e.to obtain information on being provided, provided and planned healthcare services and to enable him/her to monitor his/her status on lists of persons waiting for provision of service.

	1. **safeguarding documentation against destruction or loss,** 2. **maintaining integrity and reliability of documentation,** 3. **permanent access to documentation for authorised persons and safeguarding the data file against unauthorised access,** 4. **identification of the person providing healthcare services and the changes recorded by him/her;** 5. **disclosing documentation in XML and PDF format,** 6. **exporting all the data in XML format in a way enabling recovery of this documentation in another ICT system,** 7. **making print-outs.** **In case where the documentation kept in electronic form is to be accompanied by documentation produced in another form, including radiological images or documentation created in paper form, digital image of this documentation is produced and entered into the IT system in a way ensuring legibility, access and consistence of documentation. In case of producing a digital image documentation is provided upon the patient's request or destroyed in a way making patient's identification impossible. Recording documentation kept in electronic form consists in applying technical solutions - appropriate to the amount of data and used technology – ensuring storage, usage and reliability of documentation contained in the IT system at least until the documentation storage deadline expires (§ 82 of the Regulation).** **Documentation kept in electronic form is adequately safeguarded, if the following conditions are jointly and permanently met:** 1. **documentation is accessible only to authorised persons,** 2. **documentation is safeguarded against accidental or unauthorised destruction,** 3. **the methods and means of documentation protection have been applied, the efficiency of which at the time of their application is commonly recognised.** **Safeguarding documentation in electronic form requires in particular regular conducting of risks analysis, developing and using procedures of safeguarding documentation and its processing systems, including procedures of access and storage, applying security measures adequate to risks, regular controlling of functioning of all organisational, technical and IT safeguarding methods, as well as carrying out periodic assessment of efficiency of those methods and drawing up and executing documentation storage plans for a long period, including moving this documentation on new IT data carriers and new data formats, if it is required for ensuring continuity of access to documentation.** **Medical documentation storage periods are common for all the entities providing healthcare services. Medical documentation of a patient who died**

	due to bodily harm or poisoning is stored for the longest period, i.e. thirty years. Other documentation is stored for twenty years, and medical documentation of children up to two years of age is stored for twenty two years. X-ray images, stored outside of the patient's medical documentation, are an exception and are stored for ten years, whereas referrals for examination or doctor's orders can be destroyed after five years. The documentation storage period shall be always counted from the end of the calendar year, when a given event occurred (death, taking of a picture, execution of a referral or order) or when the latest entry was made. After the expiry of the storage period the entity providing healthcare services is obliged to destroy medical documentation in a way making the concerned patient's identification impossible, unless this medical documentation constitutes archival materials, to which the provisions of the Act of 14 July 1983 on the national archival resource and archives (unified text: Journal of Laws of 2011, No. 123, item 698 with later amendments) apply. **The Centre of Health Information Systems shall be obliged to ensure security and integrity of disclosed and received data as well as to grant data access authorisations. Pursuant to §9 of the implementing regulation to the above Act (Regulation of 14 August 2013 by the Minister of Health as regards description, minimum functionality and organisational and technical conditions of functioning of the Platform for Sharing Online Services and Resources of Digital Medical Records as well as the Electronic Platform for Collection, Analysis and Sharing of Digital Medical Records on Medical Events) the controller of systems shall, in the scope necessary for proper operation of the systems assigned to it, develop and establish, implement and exploit, monitor and review as well as maintain and improve information security management systems ensuring confidentiality, accessibility and integrity of information. The information security management system fulfils the requirements set forth in the provisions issued on the ground of Art. 18 of the Act of 17 February 2005 on informatisation of activity of entities realising public tasks for the information security management system and takes into account the provisions specified in this Article in the scope of management of information security in healthcare.**
Data integrity:	Are any specific methods used to ensure the integrity of the data? How are patients identified in the EHR? In the context of research, are anonymisation methods used and what safeguards exist for re-identification?
	Lack of specific information.
Data security:	Where are the records stored? Is there a centralised database of EHR? What security technology is being used?
	Lack of specific information.
Rights of the person/patient concerned:	How can the right of access be exercised? How can the data be corrected? Can the person enter information in his or her own EHR? What are the legal remedies available?
	The patient has the right of access to medical documentation concerning his/her health and healthcare services provided to him. **Pursuant to Art. 31 of the Act on patients' rights and the Commissioner for Patients' Rights the patient or his/her statutory representative may raise an objection to an opinion or doctor's statement[28], if the opinion or statement has influence on the patient's rights or obligations resulting from legal provisions.**

[28] Specified in Art. 2 para. 1 of the Act of 5 December 1996 on doctor's profession and dentist's profession.

Consent:	Is the system based on an opt-in approach? Is the principle of granular consent applied (with the possibility of preventing access to certain data?)? If yes, in which situations?
	The system is based on specific legal provisions regulating the principles and method of keeping medical documentation. The system is not based on the patient's consent.
Withdrawal:	Are patients able to withdraw the consent given to EHR schemes? If yes, what is the relevant procedure to withdraw such consent? What are the consequences?
	See above.
Outsourcing processing of data:	Is outsourcing common? Under what circumstances? Where is the data outsourced to? What sort of safeguards are in place?
	Outsourcing keeping medical documentation to other entities is quite common in Poland. It requires, however, development of unambiguous legal grounds specifying the principles and the method of such outsourcing, what has been recently intensively sought by the Polish Data Protection Authority. Currently, the works on the draft act concerning this issue are pending.

2. Cloud Computing, Data Mining and Profiling from both Medical Records (including EHR) and Data not specifically related to medical records.

2.1. Data Protection Issues:

Cloud computing has brought a new dimension to the way data is stored, accessed and processed. Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS), Network as a service (NaaS) are all used by services and organisations that deal with both medical data and non-medical data.

With the development of more advanced and efficient data-mining and data-querying Medical techniques (e.g NoSQL, MapReduce, Hadoop) in conjunction with increased processing power and data storage, mining data has never been more informative, easier, and cost-effective.

Healthcare is a natural sector in which to apply new technologies and methodologies, with particular impacts in epidemiology, public health, health services research, etc.

Data that can lead to the identification of a particular individual and his/her health situation is not limited to medical data *per se,* present on Electronic Health Records, but also to unsuspicious type of information.

There is a growing concern that these schemes may be implemented in manner which does not always respect the patients' confidentiality and basic rights, and in a broader context, the use of this of information may prejudice the individuals concerned.

The ability to track and monitor patients and resources enables a more efficient provision of care but may have an impact on the right to privacy of the individual concerned.

2.2. Questions: Is your legal framework providing for a regulation of Cloud Computing, Data Mining and Profiling? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	
Case-law:	
Other:	**Currently, the Bureau of the Inspector General for Personal Data Protection (GIODO Bureau) does not have specific knowledge (proved with evidence) as to whether cloud computing is carried out in the health care sector. The Inspector General for Personal Data Protection developed guidelines (so called Ten principles of use of cloud computing services by public administration) for institutions wishing to use cloud computing services.** **In Poland, cloud computing is currently permissible by law, but it is carried out mainly based on general provisions of the Act on Personal Data Protection. From the perspective of the binding legal provisions, the processing of data, in particular personal data in a cloud may be carried out only in case, where the person/entity transferring the data (cloud user) is able to establish in what processing centres (that is where such centres are located) such data will be processed. Some cloud users assure the users that personal data will be processed only in centres located in the territory of the European Union, which is supposed to mean that personal data will not be transferred to so called third countries, referred to in the Act on Personal Data Protection. However, a problem that is extremely difficult to solve is that cloud processing agreement, which would have to become a part of the data processing agreement within the meaning of Art. 31 of the Act on Personal Data Processing, should grant the data controller (i.e. cloud user) the rights of control with reference to the cloud provider, which is currently the weakest point of application of the existing provisions for the purposes of personal data processing in a cloud. Another problem poses the processing in a cloud of information constituting legally protected secrecy, among others medical secrecy, since currently the Polish law does not provide for a possibility to commission/outsource the processing of medical data (currently, the works on the draft legal regulations on this issue are pending).** **In the Polish DPA's view, currently there is a need for changing the law, but this change does not necessarily have to consist in developing a legal act on cloud computing. It would be more reasonable to adopt a solution, according to which the existence of cloud computing should be considered in currently drawn up amendments to the acts concerning privacy protection and resources security. Development of the idea of Binding Corporate Rules (BCR) might be an acceptable solution, which is already used in other EU countries. It would allow to treat an entrepreneur – cloud provider as a "trusted area of data processing".** **Today not only the Act on Personal Data Protection, but also the Directive 95/46/WE of the European Parliament and of the Council, implemented by this Act, has an extremely territorial nature, that is it refers to the processing in the territory of Poland, processing in the territory of the European Union, processing in third countries, which ensure adequate protection – everything relates to countries' level. Whereas, a reasonable solution would be to treat corporations, which implemented such Binding Corporate Rules regarding personal data processing as a kind of counterpart of countries, that is to treat Company X being cloud provider as a trusted area of data processing. This solution, which is possible, has already been reflected in the opinions of the Article 29 Working Party, but it would be new for the Polish law.**

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).

Cloud computing:	How is cloud computing regulated in your country? Which security safeguards and standards are mandatory? Are there specific requirements in order to store medical data in the cloud? How is data shared and is the sharing regulated?
	The legal issues related to cloud computing services, including personal data processed this way, and in particular sensitive data, are more and more evidently raised by practitioners and legal doctrine in Poland and Europe. It is observed that the existing solutions do not correspond to new reality and market services offered for consumer and economic entities. **For current legal solutions concerning personal data processing are too a large extent based on actual position of particular actors of the personal data processing, whereas supranational nature of cloud computing services causes that practical application of many of them becomes impossible or very difficult.**
Government:	Do governmental programmes exist to allow for increased data-mining of medical records? If yes, what are the purposes of this data mining? Are private entities allowed to access the data? Under what circumstances? What sort of techniques and technologies are being used? To what end? Are data subjects informed of this type of data-mining?
	Lack of specific information.
Private sector:	Are private entities allowed to mine medical data which they process? Under what circumstances? Can the government have access to this data?
	The basic purpose of keeping medical documentation is to allow the patient to exercise his/her right of access to documentation on his/her health or healthcare services provided to him/her. The entity providing healthcare services shall be obliged to keep, store and disclose medical documentation in a way specified in legal provisions and to ensure the protection of data contained in this documentation. It cannot, however, use this documentation for the purposes not specified in legal provisions.
Profiling:	Are the government and the private sector allowed to employ profiling methods on medical data? If yes, under what circumstances? Is it allowed to cross and correlate non-medical data with medical data?
	According to the Polish provisions on personal data protection and one of the basic principles expressed in them – the legality principle, the data processors must have a legal ground for data processing. Each operation on health data has to be performed for specific purposes and must have legal grounds, strictly specified in Art. 27 para. 2 of the Act on Personal Data Protection[29]. The Polish DPA emphasises as well the importance of the

[29] Pursuant to Art. 27 para. 2 of the Act on Personal Data Protection the processing of sensitive data shall not constitute a breach of the Act where: 1) the data subject has given his/her written consent, unless the processing consists in erasure of personal data, 2) the specific provisions of other statute provide for the processing of such data without the data subject's consent and provide for adequate safeguards, 3) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his/her consent until the establishing of a guardian or a curator, 4) processing is necessary for the purposes of carrying out the statutory objectives of churches and other religious unions, associations, foundations, and other non-profit seeking organizations or institutions with a political, scientific, religious, philosophical, or trade-union aim and provided that the processing relates solely to the members of those organizations or institutions or to the persons who have a regular contact with them in connection with their activity and subject to providing appropriate safeguards of the processed data, 5) processing relates to the data necessary to pursue a legal claim, 6) processing is necessary for the purposes of carrying out the obligations of the controller with regard to employment of his/her employees and other persons, and the scope of processing is provided by the law, 7) processing is required for the purposes of preventive

	information obligation with reference to the person being subject of profiling. Failure to fulfil this obligation may result in criminal liability (Art. 54 of the Act on Personal Data Protection[30]).

3. RFID and wireless communication technologies

3.1. Data Protection Issues:

It is common for medical devices, such as patients' tags, to possess RFID technologies in order to facilitate the transmission of the patients' data.

It can also be related to the data-mining operations previously mentioned as it is another category of information that can be used to discern meaningful patterns.

Transmission of data through radio-frequency is not limited to medical devices. Almost any smartphone uses some technology enabling to collect, and share, the user's data. For instance, via WI-FI it is possible to identify users' locations and therefore infer some of their behaviour, which in some cases can relate to health information.

3.2. Questions: Is your legal framework providing for a regulation of RFID technologies and the transfer of personal data through wireless technologies? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	General legislation on personal data protection is applied – see above.
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
RFID:	How is RFID used in hospital/clinics for (a) resource management, (b) patient care? What types of database systems (and security) are implemented in conjunction with RFID use? How are issues of access, sharing, consent etc. managed considering that RFID may be used without the patients' knowledge.
	Lack of information.
Wireless tracking technologies:	Are hospitals/clinics employing other wireless tracking technologies besides RFID? Which ones? Do they have to follow specific security requirements? Which ones?
	Lack of information.

4. Applications (Mobile)

medicine, the provision of care or treatment, where the data are processed by a health professional subject involved in treatment, other health care services, or the management of health care services and
subject to providing appropriate safeguards, 8) the processing relates to those data which were made publicly available by the data subject, 9) it is necessary to conduct scientific researches including preparations of a thesis required for graduating from university or receiving a degree; any results of scientific researches shall not be published in a way which allows identifying data subjects, 10) data processing is conducted by a party to exercise the rights and duties resulting from decisions issued in court or administrative proceedings.

[30] Art. 54. A person who, being the controller, fails to inform the data subject of its rights or to provide him/her with the information which would enable that person to benefit from the provisions of this Act, shall be liable to a fine, partial restriction of freedom or prison sentence of up to one year.

4.1. Data Protection Issues:

Information society is increasingly relying on the use of "apps" (application), most of them mobile. These apps are commonly designed to gather personal data, and in practice often process medical data.
Technologies such as multi-touch touchscreen, accelerometers or gyroscopes, ambient light sensors, GPS and cameras, and devices featuring fingerprint and biometric sensors also involve the collection of medical data.

A mobile phone application can monitor accurately physiological data, such as heartbeats, sleep patterns, fitness information.

4.2. Questions: Is your legal framework providing for a regulation of Apps and Mobile Apps? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	**General legislation on personal data protection is applied. In GIODO's view the problems related to the protection of personal data of mobile applications' users result inter alia from the fact that many such applications are developed outside the European Union, where attitudes to personal data protection are completely different.**
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Apps:	Is it allowed to use apps and mobile apps to deploy medical services and collect medical data? If yes, which type of individual/organisation can develop and employ these apps? Are there specific security requirements for these types of apps?
	Pursuant to the Polish legal provisions on personal data protection and one of the basic principles set forth in them – the legality principle, the data processors must have a legal ground for data processing. Each operation on health data has to be performed for specific purposes and must have legal grounds, strictly specified in Art. 27 para. 2 of the Act on Personal Data Protection
Institutions:	Do hospitals/clinics/labs employ apps to gather medical data? Is there a need for a medical treatment to permit the use of an app to process the medical data? Are there specific security requirements for the institutions collecting these data from the apps? Are medico-administrative data used by hospitals/clinics for management purposes?
	Lack of information.
Tracking technologies:	Do hospitals/clinics/labs employ non-medical apps and devices to track and collect data from their patients? What type of data is collected? For what purpose? Is the data identifiable? Is the data combined with medical data?
	Lack of information.
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical apps and tracking apps? If yes, what are the standards?
	Such requirement does not result directly from commonly binding legal provisions. However, the use of privacy be design is recommended by the Polish DPA in case of issuing opinions on any undertakings related to personal data processing.

Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical diagnostic? How would this be applied to fitness and daily-basis data?
	It needs to be assumed that the application of this system, collection of data related to medical diagnostic by means of medical application/application shall take place only after fulfilling of the prerequisites specified in Art. 27 para. 2 of the Act on Personal Data Protection and after informing the person about the collection of his/her data.

5. Medical Devices and Wearable Devices

5.1. Data Protection Issues:

A medical device can be defined as: 'any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application. Such a device should be intended by the manufacturer for one of a number of defined purposes, one of which is, diagnosis, prevention, monitoring, treatment or alleviation of disease' (Directive 93/42/EEC Article 1:2)

Some eHealth and mHealth devices and apps do not fall in this definition of medical devices, as can also be the case of a software working in combination with a physical device, for instance a smartphone.

5.2. Questions: Is your legal framework providing for a regulation of Medical Devices? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	**The issue of Medical Devices in Poland is regulated by the Act of 20 May 2010 on medical devices, which governs inter alia the principles of the placing on the market and putting into service of: a) Medical devices, accessories for medical devices; b) In vitro diagnostic medical devices, accessories of in vitro diagnostic medical devices; c) Active implantable medical devices; d) Systems and procedure packs consisting of medical devices – hereinafter referred to as "devices;" as well as rules governing the supervision of compliance with the principles concerning such devices and the rules of submitting reports and notifications concerning the devices in terms of their security. Art. 2 point 38 of the above Act defines a medical device as any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic or therapeutic purposes and necessary for its proper application, intended by the manufacturer to be used for human beings for the purpose of: a) Diagnosis, prevention, monitoring, treatment or alleviation of disease, b) Diagnosis, monitoring, treatment, alleviation of or compensation for an injury or handicap, c) Investigation, replacement or modification of the anatomy or of a physiological process, d) Control of conception - and which does not achieve its principal intended action in or on the human body by pharmacological, immunological or metabolic means, but which may be assisted in its function by such means.**
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
eHealth and mHealth:	Does the concept of Medical device in your country encompass services and apparels in the realm of eHealth and mHealth? What are the requirements? Should, for instance, the medical device be certified before it can be used?
	Under Art. 11 para. 1 of the above Act the devices placed on the market and put into service shall bear the CE marking. As set forth in para. 4 of the above Article the device is affixed with the CE marking following the completion of the relevant conformity assessment procedures, certifying that the device satisfies the applicable essential requirements. Pursuant to Art. 23 para. 1 of the above Act devices must meet the relevant applicable essential requirements. On the ground of Art. 26 point 2 of the above Act it is assumed that devices are compliant with the essential elements referred to in Art. 23 para. 1, in the scope in which their compliance with relevant national standards – which were adopted based on the standards published in the Official Journal of the European Union series C - was established, as standards harmonized with the Council's Directive 93/42/EEC of 14 June 1993 concerning medical devices (EC OJ L 169 of 12.07.1993, p. 1; EU OJ Polish special edition, chapter 13, v. 12, p. 82) – in case of medical devices and accessories of medical devices
Apps:	Does the concept of medical devices encompass apps? If yes, is there any regulation applicable to apps that perform medical services? Is there any regulation applicable on apps that track non-medical data that can lead to health information? If yes, what type of data?
	The concept of medical device referred to above may encompass applications (software); the Polish legal order lacks specific regulations relating to applications that perform medical services or regulations applicable to apps that track non –medical data that can lead to health information. Therefore, general provisions resulting from the provisions of the Act on medical devices and the Act on Personal Data Protection shall apply in this regard.
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical and/or wearable devices? If yes, what are the standards?
	Such requirement does not result directly from commonly binding legal provisions. However, the use of privacy be design is recommended by the Polish DPA in case of issuing opinions on any undertakings related to personal data processing.
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical treatment? How would this be applied to fitness and daily-basis data?
	It needs to be assumed that the application of this system shall take place only after fulfilling one of the prerequisites specified in Art. 27 para. 2 of the Act on Personal Data Protection (including inter alia obtaining written consent or processing is required for the purposes of preventive medicine, the provision of care or treatment, where the data are processed by a health professional subject involved in treatment, other health care services, or the management of health care services and subject to providing appropriate safeguards) and after informing the person about the collection of his/her data.

6. Internet of Things

6.1. Data Protection Issues:

Internet of things relates to common, ordinary devices that are now, and increasingly, connected to the Internet, such as cars, fridges, ovens, microwaves, etc. All of these devices can provide data that can lead to reveal information concerning one's health. A fridge can easily inform on the type of food stored and thus the diet of an individual. One of the biggest challenges of the Internet of Things is to guarantee the right to privacy and data protection in a world where every device collects, processes, analyses and transmits the data, commonly via wireless technologies.

In the realm of medical data, the issue mainly arises when crossing seemly unrelated data that can lead to health information about an individual.

6.2. Questions: Is your legal framework providing for a regulation of the Internet of Things? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	**There is no special regulation of the Internet of Things; general legal provisions apply. According to the Polish provisions on personal data protection and one of the basic principles expressed in them – the legality principle, the data processors must have a legal ground for data processing. Each operation on health data has to be performed for specific purposes and must have legal grounds, strictly specified in Art. 27 para. 2 of the Act on Personal Data Protection.**
Case-law:	
Other:	**The website of the Polish DPA contains information about the Guide to human rights for Internet users published by the Council of Europe (Strasbourg, 17 April 2014) in order to help Internet users better understand the rights online and to advise them what they can do in case of violation of these rights (http://www.giodo.gov.pl/487/id_art/7833/j/pl/).**

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Security:	What are the security standards that need to be employed by these devices when collecting personal data?
	The security standards may result from the earlier mentioned Act on medical devices.
Non-medical devices:	Are non-medical devices allowed to collect medical data, such as heart frequency? Are they allowed to cross medical data with non-medical data?
	Such collection would be permissible only after fulfilling the conditions specified in the law, i.e. the Act on medical devices, the Act on Personal Data Protection, the legislation on patients' rights and medical documentation.
Privacy by Design:	Is there any requirement to implement privacy by design in the development of connected devices? If yes, what are the standards?
	Such requirement does not result directly from commonly binding legal provisions. However, the use of privacy by design is recommended by the Polish DPA in case of issuing opinions on any undertakings related to personal data processing.

7. Electronic Doctor (online Doctor) and on-line appointments

7.1. Data Protection Issues:

The Doctor listens, talks and assesses the patient online, via a website, app, canal, sometimes including video-conference. Medical data is collected and processed, what are the security requirements and standards followed? Other websites provide for on-line appointments with doctors, which can also involve the processing of medical data.

7.2. Questions: Is your legal framework providing for a regulation of online Medical Treatment and is the on-line appointment system covered by such a framework? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	**The existing provisions do not contain specific regulation on this issue, so the general provisions shall apply.**
Case-law:	
Other:	**In 2013 the" Platform for Sharing Online Services and Resources of Digital Medical Records with entrepreneurs" was launched. It is aimed at promoting electronic communication between entrepreneurs and public entities in the healthcare sector. It also allows for electronic registration and update of registration data (e.g. a request for permission to run a pharmacy can be submitted this way), offers a possibility for entrepreneurs to submit electronically requests to the record, to keep documents in electronic form. It also promotes the use of digital signature and helps public administration in download of registration data. Within the framework of the platform universal IT tools used for keeping records and providing electronic services are provided. The legal ground for operation of the platform is Art. 6 of the Act on the healthcare information system[31]. The technical conditions of operation of the platform are specified in the implementing regulation the above Act.[32]**

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Medical treatment:	Is it allowed to perform medical treatment via online services? If yes, how should the medical services be provided? Does it have to follow the same requirements of a regular physically-present medical treatment?
	Lack of specific legal provisions.
Medical data:	How should the data collected via a medical treatment performed online be processed? Are there specific requirements? Which ones?
	Lack of specific legal provisions.

[31] Platform for Sharing Online Services and Resources of Digital Medical Records is an IT system, which allows in particular for: 1) communication of Medical Information System (MIS) with medical records in order to obtain the data processed in those records; 2) making updates of data in medical records; 3) integration of medical records; 4) disclosure of data from medical records, in the scope of granted authorizations, to service providers and payers.
2. The controller of the system of the Platform for Sharing Online Services and Resources of Digital Medical Records is the unit subordinate to the Minister of Health, competent in healthcare IT systems
3. The task of the unit referred to in para. 2 is to provide and keep the Platform for Sharing Online Services and Resources of Digital Medical Records, to manage it and to ensure security and integrity of disclosed data.

[32] The Regulation by the Minister of Health of 14 August 2013 as regards description, minimum functionality and organisational and technical conditions of functioning of the Platform for Sharing Online Services and Resources of Digital Medical Records as well as the Electronic Platform for Collection, Analysis and Sharing of Digital Medical Records on Medical Events

Other comments and technologies
Should you wish to describe any technology, feature or trend that has not been covered by the questionnaire, please feel free to use the space provided below. Where relevant, also indicate recent legislation changes, guidelines and/or case law.

PORTUGAL

QUESTIONNAIRE

The questionnaire should ideally be completed by data protection authorities, health policy authorities, professional or patient associations as well as healthcare providers: you are invited to share it as widely as possible.

Please send your replies to dataprotection@coe.int no later than 15 December 2014.

1. Mobile Health (mHealth) and Electronic Health Records (EHR)

1.1. Data Protection Issues:

This is perhaps the biggest topic sitting at the intersection of technology and data protection. Mobile health (mHealth) and Electronic Health Records (EHR) are increasingly used in healthcare systems and provisions – it is a trend that needs to be examined.

Related to the EHR, these records are more accurate, cost-effective (in terms of storage) than paper-based notes. The concept of patient controlled/accessed EHR has been implemented in varying degrees in different countries.

Furthermore, some non-medical record can still contain health information about users and it should be considered if such records ought to be treated in a similar way to EHR.

Also, should 'medical data' as defined in Recommendation N° (97) 5 on the protection of medical data cover physical tracking data, such as pedometers or fitness data and data that can lead to medical information about an individual ?

1.2. Questions: if EHR exist in your country, is your legal framework providing for a regulation of such records? If mHealth exists in your country, is your legal framework providing for a specific regulation? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	In December 2011, the Ministry of Health constituted CIC with the main goal of implementing the Patient Portal and the Professional Portal in Health Data Platform (PDS) (Order 16519/2011). The Health Data Platform (PDS) is the Portuguese EHR, a central sharing clinical information system developed by the Monitoring Committee for the Clinical Information Technology (CAIC) and the Shared Services of the Ministry of Health, EPE (SPMS), which will act as national register and allow health professionals access to relevant clinical information to users anywhere in the country, also allows direct contact between the user and their family doctor. The current EHR are covered under the general law of data protection. There is no specific regulation for mHealth
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
EHR and Medical data:	What can be considered medical data in your country? Is it solely the data relating to a person's health (state, diagnosis, prognosis, medical treatment, etc.)? Is non-medical data that leads to medical information treated the same way as medical data (for instance in terms of confidentiality requirements)? Is the EHR solely constituted of data collected in a medical context or can the individual also himself or herself add information regarding his or her health?
	At present the Portuguese citizen can also add his own health related information via the Patient portal – This remained stored in a diferent format and accessible to him/her, as well as to public hospital/GPs doctors and nurses if, and only, if he or she so chooses to give consent (online). The patient can enter your own health information (emergency contacts, medical appointments, medicines, allergies, biometrics monitoring, vital will) through Patient Portal. The patient can manage their commitments on three levels: 1) information that is made by himself; 2) clinical information placed by health professionals; 3) sharing of clinical summary to other EU countries. If the user allows access to information professionals, this is viewed differently from the clinical information recorded by the health professional
Sharing of data and Access:	Who is granted access to the EHR and how is the sharing of information (with other health care providers?) regulated? Where information is shared with pharmacists, is there a strict purpose limitation in place? How has the definition of the responsibility over the medical data been regulated?
	The user has two levels of access to data: 1) register with login and password; 2) citizen card authentication and respective pin. Being studied the inclusion of digital mobile key Access to health data by doctors and nurses is in accordance with the authorization granted by the National Data Protection Commission. At the moment the information is not accessible to other professionals beyond doctors and nurses being studied enlargement to the following professional bodies: nutritionists, psychologists and pharmacists as well as the information that they may
Data quality:	Are the principles of legitimacy, fairness and minimisation applied to medical data? How are records kept accurate? How long is the data kept for, is the specific storage period defined for the EHR?
	Data are available from the time of registration and throughout the life cycle of the user and 6 months after the death of the holder, unless a judicial process
Data integrity:	Are any specific methods used to ensure the integrity of the data? How are patients identified in the EHR? In the context of research, are anonymisation methods used and what safeguards exist for re- identification?
	Users are identified by the National Users Registry, so there are no duplicate records and incorrect information. Quality control of these data is ensured through several cross-checking mechanisms. We have a repository of anonymized clinical information. Epidemiological data without identifying the holder are available. The use of this data for research purposes are subject to the assessment of quality committees and national data protection commission.

Data security:	Where are the records stored? Is there a centralized database of EHR? What security technology is being used?
	The Health Data Platform is a system for sharing health data between different agents of care (users, NHS professionals and outside the NHS) through specific portals (Patient Portal, Professional Portal, Institutional Portal, International Portal), reliable and contextualized, from local institutions where they stay stored, creating an anonymized clinical information repository.
Rights of the person/patient concerned:	How can the right of access be exercised? How can the data be corrected? Can the person enter information in his or her own EHR? What are the legal remedies available?
	Yes, the patient can enter your own health information (emergency contacts, medical appointments, medicines, allergies, biometrics monitoring, vital will) through Patient Portal. The user can see who, when and where their clinicians data were visualized
Consent:	Is the system based on an opt-in approach? Is the principle of granular
	consent applied (with the possibility of preventing access to certain data?)? If yes, in which situations?
	Data sharing can be managed and controlled by the patient on the Patient Portal and the patient can also audit the professionals that accessed his or her information.
Withdrawal:	Are patients able to withdraw the consent given to EHR schemes? If yes, what is the relevant procedure to withdraw such consent? What are the consequences?
	At any time the patient may withdraw permission to access their data through the Patient Portal. By not allowing access to data by health professionals, the patient is to limit access to health information that may be relevant to a better diagnosis. Furthermore, since the health professionals do not have access to medical examinations can be order for repeat and thus wasting resources.
Outsourcing processing of data:	Is outsourcing common? Under what circumstances? Where is the data outsourced to? What sort of safeguards are in place?
	By way of exception and in order to fulfill some additional activities without ever having access to users data

2. Cloud Computing, Data Mining and Profiling from both Medical Records (including EHR) and Data not specifically related to medical records.to privacy of the individual concerned.

2.2. Questions: Is your legal framework providing for a regulation of Cloud Computing, Data Mining and Profiling? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Cloud computing:	How is cloud computing regulated in your country? Which security safeguards and standards are mandatory? Are there specific requirements in order to store medical data in the cloud? How is data shared and is the sharing regulated?
Government:	Do governmental programmes exist to allow for increased data-mining of medical records? If yes, what are the purposes of this data mining? Are private entities allowed to access the data? Under what circumstances? What sort of techniques and technologies are being used? To what end? Are data subjects informed of this type of data-mining?
	Yes there are increased interest in mining data for population profiling and primary care planning in the regions. A set of 100 indicators is constructed out of medical records in GP oficies to allow contracting of services. Private doctors can have access to a concise set of EHR functionality, having to identify with the credentials acquired in cental portal, the same used in the electronic medication prescription. The user must enter the citizen card together with the pin in private clinics
Private sector:	Are private entities allowed to mine medical data which they process? Under what circumstances? Can the government have access to this data?
	Yes private entities can use they data for mining as long as they follow the general data protection law. At the moment there is no sharing of information recorded in the private doctor, only if prescribe drugs electronically.
Profiling:	Are the government and the private sector allowed to employ profiling methods on medical data? If yes, under what circumstances? Is it allowed to cross and correlate non-medical data with medical data?

3. RFID and wireless communication technologies

3.1. Data Protection Issues:

It is common for medical devices, such as patients' tags, to possess RFID technologies in order to facilitate the transmission of the patients' data.

It can also be related to the data-mining operations previously mentioned as it is another category of information that can be used to discern meaningful patterns.

Transmission of data through radio-frequency is not limited to medical devices. Almost any smartphone uses some technology enabling to collect, and share, the user's data. For instance, via WI-FI it is possible to identify users' locations and therefore infer some of their behaviour, which in some cases can relate to health information.

3.2. Questions: Is your legal framework providing for a regulation of RFID technologies and the transfer of personal data through wireless technologies? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
RFID:	How is RFID used in hospital/clinics for (a) resource management, (b) patient care? What types of database systems (and security) are implemented in conjunction with RFID use? How are issues of access, sharing, consent etc. managed considering that RFID may be used without the patients' knowledge.
Wireless tracking technologies:	Are hospitals/clinics employing other wireless tracking technologies besides RFID? Which ones? Do they have to follow specific security requirements? Which ones?

4. Applications (Mobile)

4.1. Data Protection Issues:

Information society is increasingly relying on the use of "apps" (application), most of them mobile. These apps are commonly designed to gather personal data, and in practice often process medical data.
Technologies such as multi-touch touchscreen, accelerometers or gyroscopes, ambient light sensors, GPS and cameras, and devices featuring fingerprint and biometric sensors also involve the collection of medical data.

A mobile phone application can monitor accurately physiological data, such as heartbeats, sleep patterns, fitness information.

4.2. Questions: Is your legal framework providing for a regulation of Apps and Mobile Apps?
If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Apps:	Is it allowed to use apps and mobile apps to deploy medical services and collect medical data? If yes, which type of individual/organisation can develop and employ these apps? Are there specific security requirements for these types of apps?

	For the moment is not yet available. Is developing an app to view the average time in hospital emergencies.
Institutions:	Do hospitals/clinics/labs employ apps to gather medical data? Is there a need for a medical treatment to permit the use of an app to process the medical data? Are there specific security requirements for the institutions collecting these data from the apps? Are medico-administrative data used by hospitals/clinics for management purposes?
	No
Tracking technologies:	Do hospitals/clinics/labs employ non-medical apps and devices to track and collect data from their patients? What type of data is collected? For what purpose? Is the data identifiable? Is the data combined with medical data?

Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical apps and tracking apps? If yes, what are the standards?
	Yes we followed this principle by working with the data protection agency from day1 when desiging the national data sharing platform.
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical diagnostic? How would this be applied to fitness and daily-basis data?
	National project (PDS – plataforma de dados de saude – Portuguese Health record) uses a opt-out approach, except in the case of cross-border data (epSOS, EXPAND atc) where patient has to give explicit consent. Also in the case of sharing his own (recorded by him/herself) information with the NHS the consent needs to be explicit. All consents are managed online in the patient Portal.

5. Medical Devices and Wearable Devices

5.1. Data Protection Issues:

A medical device can be defined as: 'any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application. Such a device should be intended by the manufacturer for one of a number of defined purposes, one of which is, diagnosis, prevention, monitoring, treatment or alleviation of disease' (Directive 93/42/EEC Article 1:2)

Some eHealth and mHealth devices and apps do not fall in this definition of medical devices, as can also be the case of a software working in combination with a physical device, for instance a smartphone.

5.2. Questions: Is your legal framework providing for a regulation of Medical Devices? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	Designates the INFARMED - National Authority of Medicines and Health Products, IP, and national authority responsible for the evaluation of health technologies (order
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
eHealth and mHealth:	Does the concept of Medical device in your country encompass services and apparels in the realm of eHealth and mHealth? What are the requirements? Should, for instance, the medical device be certified before it can be used?
	This has not been clarified
Apps:	Does the concept of medical devices encompass apps? If yes, is there any regulation applicable to apps that perform medical services? Is there any regulation applicable on apps that track non-medical data that can lead to health information? If yes, what type of data?
	This has not been clarified.
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical and/or wearable devices? If yes, what are the standards?
	no
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical treatment? How would this be applied to fitness and daily-basis data?

6. Internet of Things

6.1. Data Protection Issues: transmits the data, commonly via wireless technologies.

In the realm of medical data, the issue mainly arises when crossing seemly unrelated data that can lead to health information about an individual.

6.2. Questions: Is your legal framework providing for a regulation of the Internet of Things? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Security:	What are the security standards that need to be employed by these devices when collecting personal data?
Non-medical devices:	Are non-medical devices allowed to collect medical data, such as heart frequency? Are they allowed to cross medical data with non-medical data?
	Is developing a project to allow health data collection through mobile devices and equipment in order to integrate these data with the PDS. The internet of things is one of the work priorities in the area of innovation in health and assurance of health promotion.
Privacy by Design:	Is there any requirement to implement privacy by design in the development of connected devices? If yes, what are the standards?

7. Electronic Doctor (online Doctor) and on-line appointments

7.1. Data Protection Issues:

The Doctor listens, talks and assesses the patient online, via a website, app, canal, sometimes including video-conference. Medical data is collected and processed, what are the security requirements and standards followed? Other websites provide for on-line appointments with doctors, which can also involve the processing of medical data.

7.2. Questions: Is your legal framework providing for a regulation of online Medical Treatment and is the on-line appointment system covered by such a framework? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	• Reinforces the implementation of the strategy for a telemedicine network in the National Health Service(Order 8445/2014). • The technical preparation of working stations to use the Telemedicine tool from PDS (Order 8443/2014). • Consulting the Living Will in PDS (Order 96/2014); • Determines that the services and facilities of the National Health Service (NHS) should increase the use of information and communication technologies in order to promote and ensure the provision of telemedicine services to users of the NHS(Order 3571/2013)
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Medical treatment:	Is it allowed to perform medical treatment via online services? If yes, how should the medical services be provided? Does it have to follow the same requirements of a regular physically-present medical treatment?
	Through the PDS (PDS Live) telemedicine consultations are held between hospital / hospital, health center / hospital, health center / user
Medical data:	How should the data collected via a medical treatment performed online be processed? Are there specific requirements? Which ones?
	The consultation takes place in a chat room in clinical context in which is provided a share audio and video as well as the possibility of screen sharing. The data are entered and performed report, which is available in the PDS

Other comments and technologies
Should you wish to describe any technology, feature or trend that has not been covered by the questionnaire, please feel free to use the space provided below. Where relevant, also indicate recent legislation changes, guidelines and/or case law.

SERBIA / SERBIE

QUESTIONNAIRE

1. Mobile Health (mHealth) and Electronic Health Records (EHR)

1.1. Data Protection Issues:

This is perhaps the biggest topic sitting at the intersection of technology and data protection. Mobile health (mHealth) and Electronic Health Records (EHR) are increasingly used in healthcare systems and provisions – it is a trend that needs to be examined.

Related to the EHR, these records are more accurate, cost-effective (in terms of storage) than paper-based notes. The concept of patient controlled/accessed EHR has been implemented in varying degrees in different countries.

Furthermore, some non-medical record can still contain health information about users and it should be considered if such records ought to be treated in a similar way to EHR.

Also, should 'medical data' as defined in Recommendation N° (97) 5 on the protection of medical data cover physical tracking data, such as pedometers or fitness data and data that can lead to medical information about an individual ?

1.2. Questions: if EHR exist in your country, is your legal framework providing for a regulation of such records? If mHealth exists in your country, is your legal framework providing for a specific regulation? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	Law on Personal Data Protection ("Official Gazette of the Republic of Serbia", Nos. 97/2008, 104/2009 - other law, 68/2012 - decision of the Constitutional Court and 107/2012), being the general law regulating personal data processing in the Republic of Serbia, shall be applied to all data controllers and the data processing actions, including the actions relating to the medical data in the electronic personal data files processed by public authorities, institutions and health care institutions. In accordance with the above, controllers of personal health data shall, pursuant to Article 48 of the Law on Personal Data Protection, establish and maintain records containing the following information: 1) Type of data and name of data file; 2) Type of processing activities; 3) Business name, name, head office and address of the controller; 4) Date of commencement of data processing or date of data file creation; 5) The purpose of processing; 6) The legal grounds for data processing or creation of data file; 7) The category of data subjects; 8) The type and degree of data confidentiality; 9) The method of data collection and keeping; 10) The time limit for data keeping and use; 11) Business name, name, head office and address of the data user; 12) The mark under which data are transferred in or out of the Republic of Serbia, with an indication of the state or international organization and the foreign data user, the legal grounds and the purpose of transborder transfer in or out of the country; 13) Safeguards put in place to protect data; 14) Requests concerning data processing. In addition, pursuant to Article 49 of the Law, before the commencement of data

	processing or creation of data files, as the case may be, controllers shall notify the Commissioner of their intent to form a data file, with the enclosed above mentioned data, as well as of any intended subsequent processing, such notification being due before the processing takes place, and in any case not later than 15 days before the formation of the data file or before data processing. The notification duty shall not apply to the commencement of data processing or creation of data files in cases where special regulations govern the purpose of processing, the type of data processed, categories of users with access to the data and the period during which such data will be retained. Pursuant to Article 51 of the Law, controllers shall submit to the Commissioner records of data files, or changes in data records at the latest within 15 days from the date of data file formation, or change. Failure to comply with the provisions of the Law on Personal Data Protection shall constitute an infringement set out in items 12) and 13), paragraph 1 of Article 57 of the Law. The following *leges speciales* govern Electronic Health Records in the health care system: -Law on Health Care ("Official Gazette of the Republic of Serbia", Nos. 107/2005, 72/2009 - other law, 88/2010, 99/2010, 57/2011, 119/2012, 45/2013 - other law and 93/2014), Article 74; -Law on Health Care Insurance ("Official Gazette of the Republic of Serbia", Nos. 107/2005, 109/2005 - corrigendum, 57/2011, 110/2012 - decision of the Constitutional Court, 119/2012, 99/2014, 123/2014 and 126/2014 - decision of the Constitutional Court); -Decree on the program of work, development and organization of the integrated health care information system - "E-HEALTH" ("Official Gazette of the Republic of Serbia", No. 55/2009); - Rulebook on the technological and functional requirements for the establishment of an integrated health care information system ("Official Gazette of the Republic of Serbia", No. 95/2009) Draft Law on Medical Documentation and Health Records in the Field of Health Care (http://www.zdravlje.gov.rs/downloads/2013/Oktobar/Oktobar2013ZakonZd.doc), which governs the medical documentation and health records in the field of health care, types and content of medical documentation and health records, the manner and procedure of maintenance, persons authorized for medical documentation maintenance and data entry, timelines for data submission and processing, manner of disposal of data contained in the patients' medical documentation used for data processing, quality assurance, data protection and keeping, and other issuer relevant to the maintenance of medical documentation and records, has been prepared and is under review. Medical documentation and health records, established pursuant to the Law, shall constitute grounds for the operation of the integrated health information system, which shall be comprised of the health-statistics system, information system of health insurance organizations and information systems of health care institutions, private practice and other legal entities. Under the Draft Law, medical documentation and health records may be maintained in written or electronic form in accordance with the law (approval-certificate), in which event the results entered in the medical documentation shall be verified via the qualified electronic signature of the person who has entered the said results. The Draft provides for the obligation of health care institutions, private practice and other legal entities, to establish an information system, which shall constitute of a comprehensive set of technology infrastructure (network, software and hardware components), organization, people and processes for the collection, filing, processing, storage, transmission, display and use of data and information. The Commissioner had repeatedly (18 July, 2014, 12 November, 2013 and 9 December, 2013) on occasion of the Draft Law on Medical Documentation and Health Records in the Field of Health Care, provided opinions for the line ministry, and tried to influence the final text of the Draft before its entry in further levels of

	the procedure. The Commissioner believes that the Draft Law is an evident positive development and a step forward in relation to the applicable legal solutions in terms of regulation of the field of health records and protection of personal data contained therein; however in addition to the above mentioned, the Commissioner has noted in particular that in the proposed text of the Draft Law it is necessary to: 1. Specify all personal data in the said records which are to be processed, and clearly define the purpose of the processing in the cases where it is not clearly defined; 2. Prescribe the security, protection and access rules in relation to the data in the said records more precisely so that the health care professionals can access the data on a need-to-know basis, i.e. unauthorized access should be prevented; 3. Define the period of keeping the documentation contained in the records precisely; 4. Prescribe the processing of personal data contained in the said records by law and avoid reference to secondary legislation.
Case-law:	N/A
Other:	The non-governmental organization (Association ''Right to Health") which has completed this questionnaire at the request of the Commissioner pointed out the lack of security standards and the legal framework governing the electronic records in the field of health care, which in practice, according to their claims, leads to free access and change of electronic records at any time, and uncontrolled and illegal sharing or information. In addition, it is stated that the data on the health status of the patient, together with other personal data, are resold to commercial companies engaged in on-line sales of assistive devices.

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
EHR and Medical data:	What can be considered medical data in your country? Is it solely the data relating to a person's health (state, diagnosis, prognosis, medical treatment, etc.)? Is non-medical data that leads to medical information treated the same way as medical data (for instance in terms of confidentiality requirements)? Is the EHR solely constituted of data collected in a medical context or can the individual also himself or herself add information regarding his or her health?
	Pursuant to item 1), Article 3 of the Law on Personal Data Protection, personal data means any information relating to a natural person, regardless of the form of its presentation or the medium used. Pursuant to Article 16 of the Law the **data relating to health status shall constitute particularly sensitive personal data**. The processing of particularly sensitive personal data shall be legal solely on the basis of the consent of data subjects or insofar as this is allowed under the law. The processing of particularly sensitive personal data should be protected by safeguards which should have been standardized under a Government decree, however the decree has not been passed to this very day. In terms of the ''treatment of non-medical data that leads to medical information'', **any data directly relating to the health status, or ''revealing or referring'' to the health status, shall constitute particularly sensitive personal data,** pursuant to the Law on Personal Data Protection. Pursuant to the program of work, development and organization of the integrated health care information system – e-health2015 (''Official Gazette of the Republic of Serbia", No. 55/09), the term ''health information'' or ''health data" shall mean any information used to adopt health decisions relating to health care, either at the personal, professional, management or decision makers' level.

	The regulations governing the establishment of certain personal data files govern the purpose of processing of the data contained in the file, as well. For example, pursuant to Articles 119 and 120 of the Law on Health Care Insurance, in the Central Registry, which is maintained by the Republican Health Care Insurance Fund on the insured in the compulsory health care insurance system of the Republic of Serbia, entered shall be the general identification data of the insured-natural person, such as the first name and family name, personal ID number, address of the place of domicile, day, month and year of birth, occupation, etc., including the type of entitlements deriving from compulsory health care insurance provided to the insured person, health care services delivered, benefits, medical-technical aids and implants, prescription medications, annual amount of paid participation, chosen physician of the insured person, exercised entitlements before medical commissions, exercised entitlements concerning work-related injuries and diseases of the insured person, referrals to a Disability Commission in accordance with the Law. Pursuant to Article 138 of the Law, the data kept in the Central Registry shall be processed solely for the purposes of compulsory health care insurance. Applicable legislation in the Republic of Serbia does not provide for a natural person to add data in the records containing the data regarding his/her health status.
Sharing of data and Access:	Who is granted access to the EHR and how is the sharing of information (with other health care providers?) regulated? Where information is shared with pharmacists, is there a strict purpose limitation in place? How has the definition of the responsibility over the medical data been regulated?
	Access to electronic records is not specifically regulated. As a rule, the records are accessed by health care professionals (physicians and nurses) in a health care institution maintaining them, via a single or group access order. Information sharing with other health care services providers and pharmaceutical companies is not regulated in a comprehensive manner. Certain laws (e.g. the Law on Protection of Population against Infectious Diseases, Law on Health Care and other laws) contain provisions which oblige health care institutions to either regularly, or incidentally, submit reports to prescribed health care institutions (e.g. public health institutes), where some of the reports contain personal data (i.e. data based on which the data subject is identified or may be identified), while others do not contain such data. The Law on Medicines and Medical Devices (‘‘Official Gazette of the Republic of Serbia“, No. 30/2010) in Article 158 obliges a marketing authorization holder (pharmaceutical company) to keep records of all suspected adverse reactions to a medicinal product, which have been reported by health care or veterinary professionals, or which he/she can reasonably be expected to be aware of, and which meet the criteria for reporting pursuant to the Law and secondary legislation adopted to implement the Law, as well as to promptly report the information to the Agency for Medicines and Medical Devices no later than 15 days following the receipt of the information. The Rulebook on the method of reporting, collecting and monitoring of adverse reactions to medicines (‘‘Official Gazette of the Republic of Serbia“, No. 64/2011), which was adopted pursuant to the above mentioned Law, in paragraph 2, Article 9 provides for a possibility for a patient to notify the marketing authorization holder (i.e. pharmaceutical company) about adverse reactions to medicines, and the report shall contain the data on the party reporting the adverse reaction, the patient that can be identified (by initials, year of birth and gender), name of the medicine that is suspected to have caused the adverse reaction (trade name, i.e. INN) and the adverse reaction to the medicine; and the

	said Rulebook in paragraph, Article 10 provides that the patient shall inform about adverse reactions to a medicine by sending a completed form by mail, electronic mail or fax. The purpose of submitting the data on patients to pharmaceutical companies in such a manner shall be, in accordance with the said legislation, to record adverse reactions to a medicine, therefore pharmaceutical companies must not process the data for other purposes, which would constitute unauthorized processing of personal data within the meaning of item 2), Article 8 of the Law on Personal Data Protection. The Criminal Code ("Official Gazette of the Republic of Serbia", Nos. 85/2005, 88/2005 - corrigendum, 107/2005 - corrigendum, 72/2009, 111/2009, 121/2012, 104/2013 and 108/2014) in Article 146 provides for criminal liability for unlawful processing of personal data. The Law on Personal Data Protection, in Article 57 provides for liability of a personal data controller, i.e. responsible or natural person, for a misdemeanor falling within the scope of the Law, where under item 5), paragraph 1 of the Law, processing of particularly sensitive personal data (which includes the health status data) contrary to the provisions of Articles 16-18 of the Law, shall constitute a misdemeanor. The Law on Patients' Rights ("Official Gazette of the Republic of Serbia", No. 45/2013), in Articles 44 and 46 provides for misdemeanor liability of a health care institution, i.e. natural person, for violating the provisions of the Law relating to the obligation to maintain the confidentiality of patients' personal data. The Law on Health Care ("Official Gazette of the Republic of Serbia", Nos. 107/2005, 72/2009 - other law, 88/2010, 99/2010, 57/2011, 119/2012, 45/2013 - other law and 93/2014) in item 14), Article 256 provides for misdemeanor liability of a health care institution, i.e. other legal entity performing healthcare activity, if it fails to maintain medical documentation pursuant to this Law, i.e. if it fails to forward individual, summary and periodic reports to the competent authority within the prescribed time period, or if it in any way violates the secrecy of data in the patients' the medical documentation, i.e. if it fails to protect medical documentation from unauthorized access, copying and misuse. The Law on Health Care Insurance ("Official Gazette of the Republic of Serbia", Nos. 107/2005, 109/2005 - corrigendum, 57/2011, 110/2012 - decision of the Constitutional Court, 119/2012, 99/2014, 123/2014 and 126/2014 - decision of the Constitutional Court) in Article 243 provides for misdemeanor liability of the Republican Health Care Insurance Fund if the data maintained in the Central Registry, pertaining to the exercise of entitlements deriving from health care insurance for the insured, are not kept separately from other data contained in the Central Registry, or if such data are entered and handled by an unauthorized official.
Data quality:	Are the principles of legitimacy, fairness and minimisation applied to medical data? How are records kept accurate? How long is the data kept for, is the specific storage period defined for the EHR?
	Medical data are governed by the general principles of personal data processing provided for by Article 8 of the Law on Personal Data Protection (legal grounds in terms of a legal authority or a data subject's consent to processing, clearly defined and admissible purpose, proportionality and appropriateness, timeliness and data accuracy, credibility of the data source, admissibility of the manner of processing), including Articles 16-18 of the Law, and special provisions of the Law governing the processing of particularly sensitive personal data pursuant to which particularly sensitive personal data may be processed on the basis of informed consent of data

	subjects, save where the law does not allow the processing of such data even with the subject's consent, and the health status data may be processed without the consent of data subjects, insofar as this is allowed under the law. Pursuant to the Draft Law on Medical Documentation and Health Records in the Field of Health Care, the following basic principles of record maintenance shall apply to the field of health care: - Principle of data quality which shall ensure that the data in the medical documentation and health records shall be usable and up-to-date from the aspect of provision of health care to patients and the aspect of health care of the population; - Principle of mandatory maintenance of medical documentation and health records shall be exercised by maintaining the documentation and records, which are a part of professional work and obligations of health care institutions, private practice and other legal entities, including the health care professionals and health care associates and other persons who are collecting and processing data, within the prescribed timelines; - Principle of proportionality and appropriateness shall ensure adequate use of the data from the medical documentation and health records for precisely stipulated purposes within the appropriate scope; - Principle of management, collection and processing of personal data shall ensure accurate collection and processing of personal data, in compliance with the measures ensuring the exercise of rights to confidentiality and privacy in accordance with the law governing the protection of personal data; - Principle of rational disposal of available resources involves the use of all available resources for the operation of health care institutions, private practice and other legal entities so as to save financial resources, focus on the provision of health care, i.e. increase the time available to work with patients, and use the information and communication technologies, as well. Certain applicable legislation (e.g. the Law on Health Care Insurance) stipulates timelines for updating and/or maintaining the data in certain data files. The Draft Law on Medical Documentation and Health Records in the Field of Health Care provides for timelines for keeping medical documentation and health records.
Data integrity:	Are any specific methods used to ensure the integrity of the data? How are patients identified in the EHR? In the context of research, are anonymisation methods used and what safeguards exist for re-identification?
	General provisions of the Law on Personal Data Protection shall apply to these issues.
Data security:	Where are the records stored? Is there a centralised database of EHR? What security technology is being used?
	Pursuant to Article 48 of the Law on Personal Data Protection, data controllers shall establish and maintain personal data processing records, and, pursuant to Article 51 of the Law, they shall submit to the Commissioner records of data files which shall be entered in the Central Register maintained by the Commissioner.

Rights of the person/patient concerned:	How can the right of access be exercised? How can the data be corrected? Can the person enter information in his or her own EHR? What are the legal remedies available?
	Pursuant to paragraph 4, Article 42 of the Constitution of the Republic of Serbia, everyone shall have the right to be informed about personal data collected about him/her, in accordance with the law, and the right to court protection in case of their abuse. Articles 19-22 of the Law on Personal Data Protection, stipulate data subjects' right to be informed of the processing and their rights relating to the processing (right of access, right to require corrections and deletion of the data, etc.). Data subjects shall have a right to appeal to the Commissioner in relation to the decision of the health care institution regarding the request of the data subject to exercise the rights set out in the said articles of the Law on Personal Data Protection . The right to examine the medical documentation is specifically set out in Article 20 of the Law on Patients' Rights, and the prevention of a person to examine medical documentation shall constitute a misdemeanor pursuant to Article 44 of the Law. Patients cannot enter the data in their health records.
Consent:	Is the system based on an opt-in approach? Is the principle of granular consent applied (with the possibility of preventing access to certain data?)? If yes, in which situations?
	Pursuant to paragraph 2, Article 16 of the Law on Personal Data Protection the health status data may be processed without the consent of data subjects, insofar as this is allowed under the law.
Withdrawal:	Are patients able to withdraw the consent given to EHR schemes? If yes, what is the relevant procedure to withdraw such consent? What are the consequences?
	Pursuant to Article 11 of the Law on Personal Data Protection data subjects shall have the right to withdraw their consent, following which data processing shall be considered inadmissible within the meaning of item 1), Article 8 of the Law. The right to consent withdrawal shall not be applicable to personal data processing by the data controller with legal authority.
Outsourcing processing of data:	Is outsourcing common? Under what circumstances? Where is the data outsourced to? What sort of safeguards are in place?
	Health care institutions contract legal entities and individuals specialized for information system maintenance, which thereby become personal data processors, within the meaning of item 8), Article 3 of the Law on Personal Data Protection. In such cases, health care institutions shall, in accordance with item 3), Article 46 of Law on Personal Data Protection, inform processors and persons who have access to data about the data confidentiality safeguards, and both the health care institution and the processor shall, pursuant to Article 47 of the Law on Personal Data Protection, take all necessary technical, HR and organizational measures, in accordance with established standards and procedures, to protect the data from being lost and damaged, from inadmissible access, modification, publication and any other abuse, and to put an obligation on data processor to ensure data confidentiality. Safeguards applied to particularly sensitive personal data, pursuant to paragraph 5, Article 16 of the Law on Personal Data Protection, shall be defined by the Government of the Republic of Serbia, upon obtaining the Commissioner's opinion; however the Government is yet to pass the said piece of legislation.

2. Cloud Computing, Data Mining and Profiling from both Medical Records (including EHR) and Data not specifically related to medical records.

2.1. Data Protection Issues:

Cloud computing has brought a new dimension to the way data is stored, accessed and processed. Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS), Network as a service (NaaS) are all used by services and organisations that deal with both medical data and non-medical data.

With the development of more advanced and efficient data-mining and data-querying Medical techniques (e.g. NoSQL, MapReduce, Hadoop) in conjunction with increased processing power and data storage, mining data has never been more informative, easier, and cost-effective.

Healthcare is a natural sector in which to apply new technologies and methodologies, with particular impacts in epidemiology, public health, health services research, etc.

Data that can lead to the identification of a particular individual and his/her health situation is not limited to medical data *per se,* present on Electronic Health Records, but also to unsuspicious type of information.

There is a growing concern that these schemes may be implemented in manner which does not always respect the patients' confidentiality and basic rights, and in a broader context, the use of this of information may prejudice the individuals concerned.

The ability to track and monitor patients and resources enables a more efficient provision of care but may have an impact on the right to privacy of the individual concerned.

2.2. Questions: Is your legal framework providing for a regulation of Cloud Computing, Data Mining and Profiling? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	This field is not specifically regulated by law. Pursuant to item 3), Article 3 of the Law on Personal Data Protection, data processing means any action taken in connection with data, and the Law explicitly stipulates: transmission, storage and disclosure through transmission, regardless whether those actions are automated, semi-automated or otherwise performed. Under Article 53 of the Law, personal data may be transferred from the Republic of Serbia to a state party to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data; data may be transferred from the Republic of Serbia to a state that is not a party to the Convention, i.e. an international organization, if such a state or international organization has a regulation or a data transfer agreement in force with provides a level of data protection equivalent to that envisaged by the Convention; and in cases of transborder transfer of data referred to in paragraph 2 of the Article, the Commissioner shall determine whether the requirements are met and safeguards put in place for the transfer of data from the Republic of Serbia and shall authorize such transfer. Data mining and profiling are also considered data processing actions within the meaning of item 3), Article 3 of the Law on Personal Data Protection and can be performed only on valid legal grounds within the meaning of item 1), Article 8 of the Law (legal authority or consent of the data subject), or special provisions of Articles 16 and 17 of the Law, if particularly sensitive personal data, including the data on health status, are being processed.
Case-law:	N/A

Other:	The said issues are not regulated under a lex specialis, and the general principles and provisions of the Constitution of the Republic of Serbia and the Law on Personal Data Protection shall apply to the said data processing actions.

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Cloud computing:	How is cloud computing regulated in your country? Which security safeguards and standards are mandatory? Are there specific requirements in order to store medical data in the cloud? How is data shared and is the sharing regulated?
	N/A
Government:	Do governmental programmes exist to allow for increased data-mining of medical records? If yes, what are the purposes of this data mining? Are private entities allowed to access the data? Under what circumstances? What sort of techniques and technologies are being used? To what end? Are data subjects informed of this type of data-mining?
	N/A
Private sector:	Are private entities allowed to mine medical data which they process? Under what circumstances? Can the government have access to this data?
	N/A
Profiling:	Are the government and the private sector allowed to employ profiling methods on medical data? If yes, under what circumstances? Is it allowed to cross and correlate non-medical data with medical data?
	Pursuant to paragraph 3, Article 42 of the Constitution of the Republic of Serbia the use of personal data for any purpose other the one they were collected for shall be prohibited and punishable in accordance with the law, unless this is necessary to conduct criminal proceedings or protect safety of the Republic of Serbia, in a manner stipulated by the law. Pursuant to item 2), Article 8 of the Law on Personal Data Protection processing of personal data shall not be allowed if processing is done for purposes other than those specified. Pursuant to paragraph 1, Article 16, the data relating to health status shall be processed on the basis of informed consent, save where the law does not allow the processing of such data even with the data subject's consent, and pursuant to paragraph 2 of the said Article the data relating to health status may be processed without the consent of data subjects, insofar as this is allowed under the law. Pursuant to paragraph 1, Article 17 of the Law consent to processing of particularly sensitive data, including the medical data, shall be given in writing and shall contain a designation of the data processed, the purpose of processing and the manner of use of such consent. Pursuant to the above mentioned constitutional and legal provisions, the health status data shall be processed only for purposes specified by law and with the consent of data subjects, insofar as this is allowed under the law.

3. RFID and wireless communication technologies

3.1. Data Protection Issues:

It is common for medical devices, such as patients' tags, to possess RFID technologies in order to facilitate the transmission of the patients' data.

It can also be related to the data-mining operations previously mentioned as it is another category of information that can be used to discern meaningful patterns.

Transmission of data through radio-frequency is not limited to medical devices. Almost any smartphone uses some technology enabling to collect, and share, the user's data. For instance, via WI-FI it is possible to identify users' locations and therefore infer some of their behaviour, which in some cases can relate to health information.

3.2. Questions: Is your legal framework providing for a regulation of RFID technologies and the transfer of personal data through wireless technologies? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	This area is not specifically regulated by law.
Case-law:	N/A
Other:	The said issues are not regulated under a lex specialis, and the general principles and provisions of the Constitution of the Republic of Serbia and the Law on Personal Data Protection shall apply to the said data processing actions.

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
RFID:	How is RFID used in hospital/clinics for (a) resource management, (b) patient care? What types of database systems (and security) are implemented in conjunction with RFID use? How are issues of access, sharing, consent etc. managed considering that RFID may be used without the patients' knowledge?
	According to the responses of an NGO which has completed the questionnaire at the request of the Commissioner, the use of RFID technology in health care institutions is limited to the access to the data about the location and presence.
Wireless tracking technologies:	Are hospitals/clinics employing other wireless tracking technologies besides RFID? Which ones? Do they have to follow specific security requirements? Which ones?
	N/A

4. Applications (Mobile)

4.1. Data Protection Issues:

Information society is increasingly relying on the use of "apps" (application), most of them mobile. These apps are commonly designed to gather personal data, and in practice often process medical data.
Technologies such as multi-touch touchscreen, accelerometers or gyroscopes, ambient light sensors, GPS and cameras, and devices featuring fingerprint and biometric sensors also involve the collection of medical data.

A mobile phone application can monitor accurately physiological data, such as heartbeats, sleep patterns, fitness information.

4.2. Questions: Is your legal framework providing for a regulation of Apps and Mobile Apps? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	This field is not specifically regulated by the law.
Case-law:	N/A

Other:	The said issues are not regulated under a lex specialis, and the general principles and provisions of the Constitution of the Republic of Serbia and the Law on Personal Data Protection shall apply to the said data processing actions.

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Apps:	Is it allowed to use apps and mobile apps to deploy medical services and collect medical data? If yes, which type of individual/organisation can develop and employ these apps? Are there specific security requirements for these types of apps?
	N/A
Institutions:	Do hospitals/clinics/labs employ apps to gather medical data? Is there a need for a medical treatment to permit the use of an app to process the medical data? Are there specific security requirements for the institutions collecting these data from the apps? Are medico-administrative data used by hospitals/clinics for management purposes?
	N/A
Tracking technologies:	Do hospitals/clinics/labs employ non-medical apps and devices to track and collect data from their patients? What type of data is collected? For what purpose? Is the data identifiable? Is the data combined with medical data?
	According to the responses of an NGO which has completed the questionnaire at the request of the Commissioner, an application for reading the barcode on the health insurance card is used.
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical apps and tracking apps? If yes, what are the standards?
	N/A
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical diagnostic? How would this be applied to fitness and daily-basis data?
	N/A

5. Medical Devices and Wearable Devices

5.1. Data Protection Issues:

A medical device can be defined as: 'any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application. Such a device should be intended by the manufacturer for one of a number of defined purposes, one of which is, diagnosis, prevention, monitoring, treatment or alleviation of disease' (Directive 93/42/EEC Article 1:2)

Some eHealth and mHealth devices and apps do not fall in this definition of medical devices, as can also be the case of a software working in combination with a physical device, for instance a smartphone.

5.2. Questions: Is your legal framework providing for a regulation of Medical Devices? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	Chapter IV of the Law on Medicines and Medical Device ("Official Gazette of the Republic of Serbia", Nos. 30/2010 and 107/2012) governs medical devices.
Case-law:	N/A
Other:	The general principles and provisions of the Constitution of the Republic of Serbia and the Law on Personal Data Protection shall apply to the personal data which are processed due to the use of medical devices.

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
eHealth and mHealth:	Does the concept of Medical device in your country encompass services and apparels in the realm of eHealth and mHealth? What are the requirements? Should, for instance, the medical device be certified before it can be used?
	The Law on Medicines and Medical Devices in Article 171 provides for and recognizes the following types of medical devices: 1) **general medical devices** (Article 172: General medical devices shall mean any instruments, apparatuses, appliances, and products intended to be used for human beings, whether they are used alone or in combination, including the software necessary for their proper application, for the purposes of: 1) diagnosis, prevention, monitoring, treatment or alleviation of disease, 2) diagnosis, monitoring, treatment and alleviation of or compensation for an injury or disability, 3) investigation, replacement or modification of the anatomy or a physiological process, 4) control of conception); 2) **in-vitro diagnostic medical devices** (Article 173: In-vitro diagnostic medical devices shall include any reagents, reagent products, control and calibration materials, reagent kits, instruments, apparatuses, equipment or systems used independently or in combination intended to be used *in-vitro* for the examination of samples derived from the human body, including human blood and tissues, in order to obtain the information: 1) concerning physiological or pathological state, 2) concerning congenital abnormalities, 3) required for determining the safety and compatibility with potential recipients, 4) required for monitoring therapeutic measures); 3) **active implantable medical devices** (Article 174: Active implantable medical devices are the products whose actions depend on the source of electricity or any other energy sources that are not powered directly from the human body or gravity, which are intended to be either totally or partially introduced into the human body by surgical intervention, or permanently introduced into a natural orifice). Pursuant to Article 177 of the Law on Medicines and Medical Devices, medical devices can be placed on the market in the Republic of Serbia only upon registration in the Register of Medical Devices. The following documents shall be submitted in order to perform the registration:

	1) Certificate of Conformity issued by the authorized Notified Body, or Declaration of Conformity; 2) Marketing Authorization for a medical device which is not compliant with the European Union Medical Device Directive.
Apps:	Does the concept of medical devices encompass apps? If yes, is there any regulation applicable to apps that perform medical services? Is there any regulation applicable on apps that track non-medical data that can lead to health information? If yes, what type of data?
	See the previous answer, please.
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical and/or wearable devices? If yes, what are the standards?
	N/A
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical treatment? How would this be applied to fitness and daily-basis data?
	N/A

6. Internet of Things

6.1. Data Protection Issues:

Internet of things relates to common, ordinary devices that are now, and increasingly, connected to the Internet, such as cars, fridges, ovens, microwaves, etc. All of these devices can provide data that can lead to reveal information concerning one's health. A fridge can easily inform on the type of food stored and thus the diet of an individual. One of the biggest challenges of the Internet of Things is to guarantee the right to privacy and data protection in a world where every device collects, processes, analyses and transmits the data, commonly via wireless technologies.

In the realm of medical data, the issue mainly arises when crossing seemly unrelated data that can lead to health information about an individual.

6.2. Questions: Is your legal framework providing for a regulation of the Internet of Things? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	This field is not specifically regulated by the law.
Case-law:	N/A
Other:	The said issues are not regulated under a lex specialis, and the general principles and provisions of the Constitution of the Republic of Serbia and the Law on Personal Data Protection shall apply to the said data processing actions.

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).

Security:	What are the security standards that need to be employed by these devices when collecting personal data?
	N/A

Non-medical devices:	Are non-medical devices allowed to collect medical data, such as heart frequency? Are they allowed to cross medical data with non-medical data?
	N/A
Privacy by Design:	Is there any requirement to implement privacy by design in the development of connected devices? If yes, what are the standards?
	N/A

7. Electronic Doctor (online Doctor) and on-line appointments

7.1. Data Protection Issues:

The Doctor listens, talks and assesses the patient online, via a website, app, canal, sometimes including video-conference. Medical data is collected and processed, what are the security requirements and standards followed? Other websites provide for on-line appointments with doctors, which can also involve the processing of medical data.

7.2. Questions: Is your legal framework providing for a regulation of online Medical Treatment and is the on-line appointment system covered by such a framework? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	This field is not specifically regulated by the law.
Case-law:	N/A
Other:	The said issues are not regulated under a lex specialis, and the general principles and provisions of the Constitution of the Republic of Serbia and the Law on Personal Data Protection shall apply to the said data processing actions.

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Medical treatment:	Is it allowed to perform medical treatment via online services? If yes, how should the medical services be provided? Does it have to follow the same requirements of a regular physically-present medical treatment?
	N/A
Medical data:	How should the data collected via a medical treatment performed online be processed? Are there specific requirements? Which ones?
	N/A

Other comments and technologies
Should you wish to describe any technology, feature or trend that has not been covered by the questionnaire, please feel free to use the space provided below. Where relevant, also indicate recent legislation changes, guidelines and/or case law.

SLOVAK REPBULIC / REPUBLIC SLOVAQUE

QUESTIONNAIRE

The questionnaire should ideally be completed by data protection authorities, health policy authorities, professional or patient associations as well as healthcare providers: you are invited to share it as widely as possible.

Please send your replies to dataprotection@coe.int no later than 15 December 2014.

1. Mobile Health (mHealth) and Electronic Health Records (EHR)

1.1. Data Protection Issues:

This is perhaps the biggest topic sitting at the intersection of technology and data protection. Mobile health (mHealth) and Electronic Health Records (EHR) are increasingly used in healthcare systems and provisions – it is a trend that needs to be examined.

Related to the EHR, these records are more accurate, cost-effective (in terms of storage) than paper-based notes. The concept of patient controlled/accessed EHR has been implemented in varying degrees in different countries.

Furthermore, some non-medical record can still contain health information about users and it should be considered if such records ought to be treated in a similar way to EHR.

Also, should 'medical data' as defined in Recommendation N° (97) 5 on the protection of medical data cover physical tracking data, such as pedometers or fitness data and data that can lead to medical information about an individual ?

1.2. Questions: if EHR exist in your country, is your legal framework providing for a regulation of such records? If mHealth exists in your country, is your legal framework providing for a specific regulation? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	Act no. 153/2013 Coll. on National Health Information System (NHIS)
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
EHR and Medical data:	What can be considered medical data in your country? Is it solely the data relating to a person's health (state, diagnosis, prognosis, medical treatment, etc.)? Is non-medical data that leads to medical information treated the same way as medical data (for instance in terms of confidentiality requirements)? Is the EHR solely constituted of data collected in a medical context or can the individual also himself or herself add information regarding his or her health?
	The NHIS is a set of health information systems used for the collection, processing and providing of information in a health service dedicated for management of health database. The NHIS is composed from several information systems like National Health Registers, National Register of Health Care Providers or National Register of Health Professionals. All these filling systems take data from other already existing filing systems (register of policyholders, register of health insurance companies, register of human medicines, database of medical devices, etc.) and in addition to other information contain personal data of individuals.

Sharing of data and Access:	Who is granted access to the EHR and how is the sharing of information (with other health care providers?) regulated? Where information is shared with pharmacists, is there a strict purpose limitation in place? How has the definition of the responsibility over the medical data been regulated?
	The National Health Information Centre (NHIC) is unique authority, responsible to provide access to NHIS through the National Health Portal (NHP). The access to NHIC is managed by principle "need to know"; ex. a list of persons to whom an access to the patient's e-Health books can be granted is stated in section 5(5) of the Act no. 153/2013. Employees of the health insurance companies have also access to the NHIS based on this principle, etc.
Data quality:	Are the principles of legitimacy, fairness and minimisation applied to medical data? How are records kept accurate? How long is the data kept for, is the specific storage period defined for the EHR?
	The Office for Personal Data Protection of the Slovak Republic (hereinafter as the "Office") is not able to answer this question at this stage because the NHIS is only in a preparatory phase and its full functionality is assumed on 1st January 2017 when the Act no. 153/2013 will fully enter into force. We expect the Office will perform only partial inspection of the NHIS implementation until this keystone.
Data integrity:	Are any specific methods used to ensure the integrity of the data? How are patients identified in the EHR? In the context of research, are anonymisation methods used and what safeguards exist for re-identification?
	The patients will be identified by secured access code, after inserting an insurance card with an electronic chip or ID card with secured electronic signature. The NHIS is only in the preparatory phase and the anonymisation methods are subject to discussion. The Office is a part of consultative procedure therefore we expect the anonymisation methods will fully meet the provisions of Slovak Act on Personal Data Protection.
Data security:	Where are the records stored? Is there a centralised database of EHR? What security technology is being used?
	The NHIS is a centralised database and takes data from many of other databases. The Office does not control technical aspects of this filing system but we are sure it will use the latest security technology taking into account sensitivity of data to be processed.
Rights of the person/patient concerned:	How can the right of access be exercised? How can the data be corrected? Can the person enter information in his or her own EHR? What are the legal remedies available?
	The right of access is performed directly by data subject having a direct access to processed data and possibility to make some own correction of processed data. The Office enters into relations between data subject and controller only in case when the controller refuse to handle correctly with data subject request and lodge a complaint against such treatment at the Office.
Consent:	Is the system based on an opt-in approach? Is the principle of granular consent applied (with the possibility of preventing access to certain data?)? If yes, in which situations?
	Yes, the NHIS is based on an opt-in approach. The scope of data to which the data subject has a right of access is stated in section 5(4) of the Act no. 153/2013. As mentioned above, the access of other stakeholders is performed on the "need to know" principle.
Withdrawal:	Are patients able to withdraw the consent given to EHR schemes? If yes, what is the relevant procedure to withdraw such consent? What are the consequences?
	The schemes of the NHIS come out from national legislation and so data subject is not allowed to withdraw the consent. He/she can only take care about accuracy of

	data. The scope of data the data subject (patient) is allowed to correct is strictly defined by of the Act no. 153/2013.
Outsourcing processing of data:	Is outsourcing common? Under what circumstances? Where is the data outsourced to? What sort of safeguards are in place?
	The NHIS uses data from many national databases (filing systems); ex. Population Register, Business Register or Trade Register, etc., as well as those already mentioned above. All these databases are operated by other public authorities or private companies. If we take all this in consideration we can state the data in NHIS is fully outsourced. The NHIS is operated by NHIC and we can expect some services will be outsourced as well. On the other hand, outsourcing can be performed only on the agreement basis between the controller (NHIC) and processor (provider of outsourcing). The clauses on personal data protection have to be incorporated into the agreement between them. The processor is fully responsible for and have to comply with provisions on data protection.

2. Cloud Computing, Data Mining and Profiling from both Medical Records (including EHR) and Data not specifically related to medical records.

2.1. Data Protection Issues:

Cloud computing has brought a new dimension to the way data is stored, accessed and processed. Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS), Network as a service (NaaS) are all used by services and organisations that deal with both medical data and non-medical data.

With the development of more advanced and efficient data-mining and data-querying Medical techniques (e.g NoSQL, MapReduce, Hadoop) in conjunction with increased processing power and data storage, mining data has never been more informative, easier, and cost-effective.

Healthcare is a natural sector in which to apply new technologies and methodologies, with particular impacts in epidemiology, public health, health services research, etc.

Data that can lead to the identification of a particular individual and his/her health situation is not limited to medical data *per se,* present on Electronic Health Records, but also to unsuspicious type of information.

There is a growing concern that these schemes may be implemented in manner which does not always respect the patients' confidentiality and basic rights, and in a broader context, the use of this of information may prejudice the individuals concerned.

The ability to track and monitor patients and resources enables a more efficient provision of care but may have an impact on the right to privacy of the individual concerned.

2.2. Questions: Is your legal framework providing for a regulation of Cloud Computing, Data Mining and Profiling? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	Act no. 122/2013 Coll. on Personal Data Protection Decree no. 55/2014 on IT systems in public sector
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).

Cloud computing:	How is cloud computing regulated in your country? Which security safeguards and standards are mandatory? Are there specific requirements in order to store medical data in the cloud? How is data shared and is the sharing regulated?
	The cloud computing is not specially regulated in relation to data processing in Slovakia. We apply only general provision stated in Act no. 122/2013 and Decree no. 55/2014 on IT systems in public sector which provide security standards for IT systems. This decree will be the basis for future act on cloud computing in public sector. The NHIS is the filing system operated by public authority in which many of sensitive data will be processed. The Slovak public authorities do not use cloud computing for any database and so we do not suppose the health data will be processed in such manner.
Government:	Do governmental programmes exist to allow for increased data-mining of medical records? If yes, what are the purposes of this data mining? Are private entities allowed to access the data? Under what circumstances? What sort of techniques and technologies are being used? To what end? Are data subjects informed of this type of data-mining?
	It is not possible to answer the question of data-mining at this stage. All e-Government databases are introduced with a noble objective but we are witness that many times it turns to other way. We live in a global information society and all filing systems are aimed to the best using of data. The data from the NHIS will be used equally by both, public authorities and private sector stakeholders. It is the matter of the Office competencies to monitor the data processing and care about personal data protection in the best possible manner. For ex. we have one state health insurance company and two private insurance companies in Slovakia. All of them use data from health filing systems to optimisation of their health care expenses by identification the groups of risky patients, elimination of usage of medicaments, limitation of doctor's capacity, etc. To achieve this aim in the best possible way they have to use all available data so the data-mining become a usual working method nowadays.
Private sector:	Are private entities allowed to mine medical data which they process? Under what circumstances? Can the government have access to this data?
	All private entities acting at health care area have access to medical data. Pursuant to Act no. 122/2013 they are not allowed to process personal data for several purposes without consent of data subject or if it is not mentioned in a special law. On the other hand, the Office discloses the usage of data for different purposes on a regular basis. The government has the access to medical data through the Ministry of Health, the Healthcare Surveillance Authority or Ministry of Finances in the anonymized way.
Profiling:	Are the government and the private sector allowed to employ profiling methods on medical data? If yes, under what circumstances? Is it allowed to cross and correlate non-medical data with medical data?
	The profiling is generally forbidden by Act no. 122/2013 but the Office discloses many times the profiling as a working method.

3. RFID and wireless communication technologies

3.1. Data Protection Issues:

It is common for medical devices, such as patients' tags, to possess RFID technologies in order to facilitate the transmission of the patients' data.

It can also be related to the data-mining operations previously mentioned as it is another category of information that can be used to discern meaningful patterns.

Transmission of data through radio-frequency is not limited to medical devices. Almost any smartphone uses some technology enabling to collect, and share, the user's data. For instance, via WI-FI it is possible to identify users' locations and therefore infer some of their behaviour, which in some cases can relate to health information.

3.2. Questions: Is your legal framework providing for a regulation of RFID technologies and the transfer of personal data through wireless technologies? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	Act no. 153/2013 Coll. on National Health Information System
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
RFID:	How is RFID used in hospital/clinics for (a) resource management, (b) patient care? What types of database systems (and security) are implemented in conjunction with RFID use? How are issues of access, sharing, consent etc. managed considering that RFID may be used without the patients' knowledge.
	We stated above the NHIS is only in the preparatory phase but Act no. 53/29013 anticipates the introduction of Health Insurance Cards (HIC) with electronic chip which can be consider as RFID. In addition, Slovakia is introducing the ID cards with secured electronic signature. The HIC will be fully introduced in 2017 and will be used for all purposes of health care, either in hospitals, clinics, health insurance companies or in front of public authorities. In general, sharing of access or using the HIC without consent of data subject is forbidden. The data subject (patient) is furthermore fully responsible to protect his/her ID cards especially against loss.
Wireless tracking technologies:	Are hospitals/clinics employing other wireless tracking technologies besides RFID? Which ones? Do they have to follow specific security requirements? Which ones?
	This is not question at this stage as the NHIS is not fully working and public hospitals/clinics do not employ the tracking technologies. The private hospitals/clinics have other possibilities how to track their clients.

4. Applications (Mobile)

4.1. Data Protection Issues:

Information society is increasingly relying on the use of "apps" (application), most of them mobile. These apps are commonly designed to gather personal data, and in practice often process medical data.
Technologies such as multi-touch touchscreen, accelerometers or gyroscopes, ambient light sensors, GPS and cameras, and devices featuring fingerprint and biometric sensors also involve the collection of medical data.

A mobile phone application can monitor accurately physiological data, such as heartbeats, sleep patterns, fitness information.

4.2. Questions: Is your legal framework providing for a regulation of Apps and Mobile Apps? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	Act no. 122/2013 Coll. on Personal Data Protection
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Apps:	Is it allowed to use apps and mobile apps to deploy medical services and collect medical data? If yes, which type of individual/organisation can develop and employ these apps? Are there specific security requirements for these types of apps?
	The personal data can be process on basis of the data subject consent, pursuant to international convention binding for the Slovak Republic or special law. Using of mobile apps does not fall upon any mentioned law category so only data subject consent can be applied. It is up to data subject whether he/she will use mobile apps or not. The Slovak Republic has no specific legal security requirements for mobile apps and so we apply ISO standards to this issue. Further, the Office seeks to apply all recommendation of Article 29 Working Party in relation to security requirements however as those apps are developed by transnational companies the application of this approach is difficult.
Institutions:	Do hospitals/clinics/labs employ apps to gather medical data? Is there a need for a medical treatment to permit the use of an app to process the medical data? Are there specific security requirements for the institutions collecting these data from the apps? Are medico-administrative data used by hospitals/clinics for management purposes?
	We are not aware of this at this time.
Tracking technologies:	Do hospitals/clinics/labs employ non-medical apps and devices to track and collect data from their patients? What type of data is collected? For what purpose? Is the data identifiable? Is the data combined with medical data?
	We are not aware of this at this time.
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical apps and tracking apps? If yes, what are the standards?
	The application of this approach is not easy for the Office as mentioned above. There are not so many Slovak companies developing apps for medical purposes.
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical diagnostic? How would this be applied to fitness and daily-basis data?
	The Office has no relevant information.

5. Medical Devices and Wearable Devices

5.1. Data Protection Issues:

A medical device can be defined as: 'any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application. Such a device should be intended by the manufacturer for one of a number of defined purposes, one of which is, diagnosis, prevention, monitoring, treatment or alleviation of disease' (Directive 93/42/EEC Article 1:2)

Some eHealth and mHealth devices and apps do not fall in this definition of medical devices, as can also be the case of a software working in combination with a physical device, for instance a smartphone.

5.2. Questions: Is your legal framework providing for a regulation of Medical Devices? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	Act no. 362/2011 Coll. on Medicaments and Health Devices
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
eHealth and mHealth:	Does the concept of Medical device in your country encompass services and apparels in the realm of eHealth and mHealth? What are the requirements? Should, for instance, the medical device be certified before it can be used?
	The no. 362/2011 defines complexly introduction of medicaments and health devices into the Slovak market. Every medicament or device has to pass a certification of national certification authority before its introduction to the market.
Apps:	Does the concept of medical devices encompass apps? If yes, is there any regulation applicable to apps that perform medical services? Is there any regulation applicable on apps that track non-medical data that can lead to health information? If yes, what type of data?
	The mobile apps are not subject of Act no. 362/2011 and they are not regulated at this time.
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical and/or wearable devices? If yes, what are the standards?
	The privacy by design is an issue of last years if not only moths. There are no special national standards to this issue in Slovakia so the Office will apply international standards in this matter.
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical treatment? How would this be applied to fitness and daily-basis data?
	We have no relevant information to this issue at this time.

6. Internet of Things

6.1. Data Protection Issues:

Internet of things relates to common, ordinary devices that are now, and increasingly, connected to the Internet, such as cars, fridges, ovens, microwaves, etc. All of these devices can provide data that can lead to reveal information concerning one's health. A fridge can easily inform on the type of food stored and thus the diet of an individual. One of the biggest challenges of the Internet of Things is to guarantee the right to privacy and data protection in a world where every device collects, processes, analyses and transmits the data, commonly via wireless technologies.

In the realm of medical data, the issue mainly arises when crossing seemly unrelated data that can lead to health information about an individual.

6.2. Questions: Is your legal framework providing for a regulation of the Internet of Things? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	Act no. 122/2013 Coll. on Personal Data Protection

Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Security:	What are the security standards that need to be employed by these devices when collecting personal data?
	The controller has to meet provisions of Chapter two of the Act no. 122/2013.
Non-medical devices:	Are non-medical devices allowed to collect medical data, such as heart frequency? Are they allowed to cross medical data with non-medical data?
	All such devices can process personal data only on the base of data subject consent. This consent has to be freely given, explicit and intelligible expressed. If data subject agrees with collection of his/her medical data by any non-medical device the Office has no power to ban it. The crossing of any data is generally forbidden.
Privacy by Design:	Is there any requirement to implement privacy by design in the development of connected devices? If yes, what are the standards?
	We have no relevant information to this issue at this time.

7. Electronic Doctor (online Doctor) and on-line appointments

7.1. Data Protection Issues:

The Doctor listens, talks and assesses the patient online, via a website, app, canal, sometimes including video-conference. Medical data is collected and processed, what are the security requirements and standards followed? Other websites provide for on-line appointments with doctors, which can also involve the processing of medical data.

7.2. Questions: Is your legal framework providing for a regulation of online Medical Treatment and is the on-line appointment system covered by such a framework? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	Act no. 122/2013 Coll. on Personal Data Protection
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Medical treatment:	Is it allowed to perform medical treatment via online services? If yes, how should the medical services be provided? Does it have to follow the same requirements of a regular physically-present medical treatment?
	The Office is aware of web pages providing online medical treatment. This is possible only on the data consent basis at this time and Slovakia has no special legislation to this issue. We apply only general data protection provision stated in the Act no. 122/2013.
Medical data:	How should the data collected via a medical treatment performed online be processed? Are there specific requirements? Which ones?
	As stated above, we have no special requirements to this issue and the controller (doctor/hospital/clinic) is obliged to fully respect the provisions of the Act no. 122/2013.

Other comments and technologies
Should you wish to describe any technology, feature or trend that has not been covered by the questionnaire, please feel free to use the space provided below. Where relevant, also indicate recent legislation changes, guidelines and/or case law.
N/A

SLOVENIA / SLOVENIE

QUESTIONNAIRE

The questionnaire should ideally be completed by data protection authorities, health policy authorities, professional or patient associations as well as healthcare providers: you are invited to share it as widely as possible.

Please send your replies to dataprotection@coe.int no later than 15 December 2014.

1. Mobile Health (mHealth) and Electronic Health Records (EHR)

1.1. Data Protection Issues:

This is perhaps the biggest topic sitting at the intersection of technology and data protection. Mobile health (mHealth) and Electronic Health Records (EHR) are increasingly used in healthcare systems and provisions – it is a trend that needs to be examined.

Related to the EHR, these records are more accurate, cost-effective (in terms of storage) than paper-based notes. The concept of patient controlled/accessed EHR has been implemented in varying degrees in different countries.

Furthermore, some non-medical record can still contain health information about users and it should be considered if such records ought to be treated in a similar way to EHR.

Also, should 'medical data' as defined in Recommendation N° (97) 5 on the protection of medical data cover physical tracking data, such as pedometers or fitness data and data that can lead to medical information about an individual ?

1.2. Questions: if EHR exist in your country, is your legal framework providing for a regulation of such records? If mHealth exists in your country, is your legal framework providing for a specific regulation? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	There is no special law on EHR. However we are in the middle of preparation of a new law – "Healthcare Databases Act" (HDA). One of the draft versions of the HDA included a new database called "eMedical Record" on central (national) level, but the idea was later abandoned due to disproportionate interference with patient`s privacy and practical inability to implement the project in the next 10 years. Otherwise HDA will provide legal basis for various eHealth projects, such as ePrescription, eAppointment, TeleStroke, eTriage and eCommunications. HDA will be implemented within 3-4 months. By the HDR the Central Registry of Patient`s Data (CRPD) shall be established in the future. CRPD is actually the system that is very close to central EHR, but certainly not in the way as the system works in Finland for instance. Some parts of CRPD (exchange of some important documents between healthcare institutions) are already working. CRPD will be extended to some other medical documents and to central database of Patient Summary data and data on the most important medical treatment of a patient for the last 6 months. EHR on local basis can be established without special legal basis or special conditions set by the law. Healthcare institution must follow general rules on personal data protection & data security. All breaches of law are sanctioned as misdemeanors.

	The “Protection of Documents and Archives and Archival Institutions Act” sets the conditions for digitalization of medical documentation (this is a form of local EHR). In practice, only few medical institutions established digitalization of a smaller part of medical documentation.
Case-law:	Few months ago Information commissioner issued negative opinion No. 0712-1/2014/2550 on the project “ePrescription” as a central national database for the purpose of prescribing and dispensing medicines, due to lack of legal basis.
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs’ opinions and/or case law).	
EHR and Medical data:	What can be considered medical data in your country? Is it solely the data relating to a person’s health (state, diagnosis, prognosis, medical treatment, etc.)? Is non-medical data that leads to medical information treated the same way as medical data (for instance in terms of confidentiality requirements)? Is the EHR solely constituted of data collected in a medical context or can the individual also himself or herself add information regarding his or her health?
	Non-medical data that leads to medical information is treated the same way as medical data, e.g. point 19 para 6 of the Personal Data protection Act (hereinafter PDPA): “biometric characteristics are also sensitive personal data if their use makes it possible to identify an individual in connection with any of the aforementioned circumstances.” Patient`s Rights Act adopted very broad definition of medical or better health data: *“every information known to healthcare personnel or other personnel within the healthcare institution, particularly information about patient`s state of health (for instance diagnosis, reasons and consequences of a certain disease or injuries), patient`s personal, family and social conditions (anamnesis), and information relating to determining, treatment or monitoring of disease or injury”* (generally called as “information on health status”).
Sharing of data and Access:	Who is granted access to the EHR and how is the sharing of information (with other health care providers?) regulated? Where information is shared with pharmacists, is there a strict purpose limitation in place? How has the definition of the responsibility over the medical data been regulated?
	Strict purpose limitation is a necessary requirement by the PDPA in all personal data processing. Exchange of medical data between healthcare institutions (and within the same healthcare institution) is generally allowed, if use of data is (by the medical or healthcare standards) necessary for the implementation of health care for an individual patient (Patient`s Rights Act). These rules apply to medical documentation in paper and electronic form (for instance local EHR). Pharmacist has access to the following personal data when dealing with concrete patient: various identification numbers, name and surname, address, health insurance, general data on a doctor, who prescribed a medicine, genera data on personal general practitioner, prescribed medicine, usage of other prescribed and issued medicines, data linked to the prescribed medicine (especially allergies, quantity, dosage, strength, instructions to pharmacist, alerts, restrictions on prescribing, drug interactions, type of prescription). Similar applies to the medicinal products.
Data quality:	Are the principles of legitimacy, fairness and minimisation applied to medical data?

	How are records kept accurate? How long is the data kept for, is the specific storage period defined for the EHR?
	Principles of legitimacy, fairness and minimisation are applied also to medical data. In practice, medical records are generally kept accurate, except some data on status of a patient - occupation, education and patient`s relatives. General retention periods are: -10 years after death of a patient (for the most important parts of medical documentation); - permanent (for dental records) and - 15 years after the creation or amendment of a document (for other, less important documentation). In 2014 minister of health prescribed more differentiated retention periods for various groups of certain medical documentation, ranging from 6 months to permanent (archival records). Local EHR must be kept in the same way as mentioned above.
Data integrity:	Are any specific methods used to ensure the integrity of the data? How are patients identified in the EHR? In the context of research, are anonymisation methods used and what safeguards exist for re-identification?
	No specific methods are set by the law, with one exception – when health data are sent (transferred) using a telecommunication means, integrity of data is provided by obligatory usage of safe digital signature. In local EHRs patients are identified by the following identity data: name, surname, address, date of birth, Internal Identification Number, Number of Health Insurance and also National Identification Number. Anonymization is not necessary for internal research projects. In other research activities anonymization must be irreversible.
Data security:	Where are the records stored? Is there a centralized database of EHR? What security technology is being used?
	Medical record must be stored according to general principles of data security set by the PDPA and internal rules, prescribed by every healthcare institution. There is no centralized database of EHR. Only local EHRs exist, BUT THESE SYSTEMS DO NOT FULLY REPLACE “CLASSIC” MEDICAL RECORDS IN PAPER FORM. These systems include only part of the data, otherwise kept in medical records.
Rights of the person/patient concerned:	How can the right of access be exercised? How can the data be corrected? Can the person enter information in his or her own EHR? What are the legal remedies available?
	Patient`s Rights Act provide the rules on access: - patient is granted (monitored) insight, paper copy, other reproduction of digital documentation or print; - right is not limited (there are some specific constitutional limitations in practice, if the access would result in a violation of children 's rights and interests); - access can be performed also by patient`s legal representatives; - healthcare institution must make decision in 5 days;

	- in case of a denial, patient has the right to appeal to the Information Commissioner. Information Commissioner decide (in a form of an administrative decision), if a patient can get access or not. Patient has the right to demand correction of identity, general, technical and status data, however patient has no right to change or delete medical data, such as diagnosis. On the other hand, patient has a right to add his own personal statement on the contents of medical records. Healthcare institutions do not allow direct computerized access to local EHRs. Patients are also not allowed to enter personal data.
Consent:	Is the system based on an opt-in approach? Is the principle of granular consent applied (with the possibility of preventing access to certain data?)? If yes, in which situations?
	Consent is needed only for the processing of data that has no legal basis in a PDPA or other law. Planned system of the Central Registry of Patient`s Data (CRPD) (legal basis shall be the new HDA), will be partially based on opt-out approach. Opt-out will not be allowed for the most important nonmedical personal data.
Withdrawal:	Are patients able to withdraw the consent given to EHR schemes? If yes, what is the relevant procedure to withdraw such consent? What are the consequences?
	As a general rule, every consent is revocable and must be fully followed. Revocation shall be made in the same way (form) as consent. No special rules on procedure exist though.
Outsourcing processing of data:	Is outsourcing common? Under what circumstances? Where is the data outsourced to? What sort of safeguards are in place?
	Outsourcing is common and widespread, but only for some individual parts of processing (for example keeping and maintenance) Data controller may by CONTRACT entrust individual tasks related to processing of personal data to data processor that is registered to perform such activities and ensures the appropriate procedures and measures for safety. Data processor may perform individual tasks associated with processing of personal data within the scope of the client's authorisations, and may not process personal data for any other purpose. Mutual rights and obligations shall be arranged by contract, which must be concluded in writing. General data security provisions (these apply to all processing of personal data) are: Security of personal data comprises organisational, technical and logical-technical procedures and measures to protect personal data, and to prevent accidental or deliberate unauthorised destruction, modification or loss of data, and unauthorised processing of such data: 1. by protecting premises, equipment and systems software, including input-output units; 2. by protecting software applications used to process personal data; 3. by preventing unauthorised access to personal data during transmission thereof, including transmission via telecommunications means and networks; 4. by ensuring effective methods of blocking, destruction, deletion or anonymisation of personal data; 5. by enabling subsequent determination of when individual personal data were entered into a filing system, used or otherwise processed, and who did so, for the period covered by statutory protection of the rights of an individual due to unauthorised supply or processing of personal data.

2. Cloud Computing, Data Mining and Profiling from both Medical Records (including EHR) and Data not specifically related to medical records.

2.1. Data Protection Issues:

Cloud computing has brought a new dimension to the way data is stored, accessed and processed. Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS), Network as a service (NaaS) are all used by services and organisations that deal with both medical data and non-medical data.

With the development of more advanced and efficient data-mining and data-querying Medical techniques (e.g NoSQL, MapReduce, Hadoop) in conjunction with increased processing power and data storage, mining data has never been more informative, easier, and cost-effective.

Healthcare is a natural sector in which to apply new technologies and methodologies, with particular impacts in epidemiology, public health, health services research, etc.

Data that can lead to the identification of a particular individual and his/her health situation is not limited to medical data *per se,* present on Electronic Health Records, but also to unsuspicious type of information.

There is a growing concern that these schemes may be implemented in manner which does not always respect the patients' confidentiality and basic rights, and in a broader context, the use of this of information may prejudice the individuals concerned.

The ability to track and monitor patients and resources enables a more efficient provision of care but may have an impact on the right to privacy of the individual concerned.

2.2. Questions: Is your legal framework providing for a regulation of Cloud Computing, Data Mining and Profiling? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	Cloud computing is not regulated per se in legislation.
Case-law:	
Other:	DPA guidelines on cloud computing: https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Cloud_computing_and_data_protection_-_ENG_final.pdf

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Cloud computing:	How is cloud computing regulated in your country? Which security safeguards and standards are mandatory? Are there specific requirements in order to store medical data in the cloud? How is data shared and is the sharing regulated?
	Cloud computing is not regulated per se in our legislation. DPA issued guidelines on cloud computing, the transfer of sensitive personal data (which includes medical data) to public clouds is advised against. Working Party opinion and IWGDPT opinion ("Sopot Memorandum") on cloud computing are also worth looking into. Sopot memorandum inter alia recommends that: 1. CC implementation should take place in careful, measured steps, starting with non-sensitive and non-confidential information. It is best to start with non-personal data. 2. Thus, CC should not be used for the processing of sensitive personal data at the present time

Government:	Do governmental programmes exist to allow for increased data-mining of medical records? If yes, what are the purposes of this data mining? Are private entities allowed to access the data? Under what circumstances? What sort of techniques and technologies are being used? To what end? Are data subjects informed of this type of data-mining?
	Not to our knowledge.
Private sector:	Are private entities allowed to mine medical data which they process? Under what circumstances? Can the government have access to this data?
	Not to our knowledge. Private sector would need appropriate legal ground – i.e. informed and explicit consent of the individual to be able to do that. Government is a broad term and can cover law enforcement, medical institutions, research centers etc.; hence it is not possible to provide a simple answer as different government bodies are governed by different legal grounds. Access to data would depend on specific circumstances of the case and concrete legal ground.
Profiling:	Are the government and the private sector allowed to employ profiling methods on medical data? If yes, under what circumstances? Is it allowed to cross and correlate non-medical data with medical data?
	Private sector would need appropriate legal ground – i.e. informed and explicit consent of the individual to be able to do that, public sector would need explicit legal ground in an act. Under these conditions also "cross and correlate non-medical data with medical data" is allowed. For example National Institute for Public Health has a rather "powerfull" legal basis to perform all kind of analytics on a national level, using a personal (not only statistical or anonymized) health data, sent by almost all health care institutions.

3. RFID and wireless communication technologies

3.1. Data Protection Issues:

It is common for medical devices, such as patients' tags, to possess RFID technologies in order to facilitate the transmission of the patients' data.

It can also be related to the data-mining operations previously mentioned as it is another category of information that can be used to discern meaningful patterns.

Transmission of data through radio-frequency is not limited to medical devices. Almost any smartphone uses some technology enabling to collect, and share, the user's data. For instance, via WI-FI it is possible to identify users' locations and therefore infer some of their behaviour, which in some cases can relate to health information.

3.2. Questions: Is your legal framework providing for a regulation of RFID technologies and the transfer of personal data through wireless technologies? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	RFID is not regulated per se in our legislation.
Case-law:	
Other:	An RFID Privacy Impact Framework was produced in EU. See: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_annex_en.pdf

	Slovenian Information Commissioner has issued some opinions on the use of RFID in certain cases. The opinions are in Slovenian only. In opinion no. 0712-1/2011/408 the Information Commissioner was asked for an opinion about the use of RFID bracelets to be worn by patients in neurological clinics, retirement homes, health clinics taking care of people with dementia and similar in order to trigger alarms when patients would cross certain virtual borders in these institutions. In its opinion the Commissioner warned that privacy by design should be implemented and that appropriate legal grounds (which could be different in different use case scenarios) and other safeguards are needed to operate such a system.

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
RFID:	How is RFID used in hospital/clinics for (a) resource management, (b) patient care? What types of database systems (and security) are implemented in conjunction with RFID use? How are issues of access, sharing, consent etc. managed considering that RFID may be used without the patients' knowledge.
	To our knowledge there are not many implementations of RFID technology in our health sector. There are some tendencies of healthcare institutions (not only in special healthcare institutions, but also in hospitals of general practice) to establish location control of their patients using a RFID bracelet. Information Commissioner allows using such devices only in emergency situations. Private idea of introducing RFID Bracelet as a key to access to patient`s centrally stored health data (patient summary) was not implemented due to lack of interest by the healthcare institutions.
Wireless tracking technologies:	Are hospitals/clinics employing other wireless tracking technologies besides RFID? Which ones? Do they have to follow specific security requirements? Which ones?
	Not to our knowledge.

4. Applications (Mobile)

4.1. Data Protection Issues:

Information society is increasingly relying on the use of "apps" (application), most of them mobile. These apps are commonly designed to gather personal data, and in practice often process medical data.
Technologies such as multi-touch touchscreen, accelerometers or gyroscopes, ambient light sensors, GPS and cameras, and devices featuring fingerprint and biometric sensors also involve the collection of medical data.

A mobile phone application can monitor accurately physiological data, such as heartbeats, sleep patterns, fitness information.

4.2. Questions: Is your legal framework providing for a regulation of Apps and Mobile Apps? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	Apps and Mobile Apps are not regulated per se in our legislation.
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Apps:	Is it allowed to use apps and mobile apps to deploy medical services and collect medical data? If yes, which type of individual/organisation can develop and employ these apps? Are there specific security requirements for these types of apps?
	To our knowledge there are not many implementations of apps and mobile apps to deploy medical services and collect medical data by data controllers in our country. Also there are not many providers of such apps in our country. Individuals may be using apps that they download themselves. General data protection rules would apply for data controllers form our country that would process personal data collected through the use of apps/mobile apps.
Institutions:	Do hospitals/clinics/labs employ apps to gather medical data? Is there a need for a medical treatment to permit the use of an app to process the medical data? Are there specific security requirements for the institutions collecting these data from the apps? Are medico-administrative data used by hospitals/clinics for management purposes?
	Gathering of data through apps is done in several projects on a small scale and strictly with the consent of a patient.
Tracking technologies:	Do hospitals/clinics/labs employ non-medical apps and devices to track and collect data from their patients? What type of data is collected? For what purpose? Is the data identifiable? Is the data combined with medical data?
	Gathering of data through apps is done in several projects on a small scale and strictly with the consent of a patient. Projects were mainly dealing with monitoring patients with chronic disease and therefore were monitoring vital signs (mainly blood pressure, saturation, other parameters were sent by the patient – typed into the application).
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical apps and tracking apps? If yes, what are the standards?
	Not to our knowledge.
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical diagnostic? How would this be applied to fitness and daily-basis data?
	According to present legislation, apps can be based on the consent of an individual.

5. Medical Devices and Wearable Devices

5.1. Data Protection Issues:

A medical device can be defined as: 'any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application. Such a device should be intended by the manufacturer for one of a number of defined purposes, one of which is, diagnosis, prevention, monitoring, treatment or alleviation of disease' (Directive 93/42/EEC Article 1:2)

Some eHealth and mHealth devices and apps do not fall in this definition of medical devices, as can also be the case of a software working in combination with a physical device, for instance a smartphone.

5.2. Questions: Is your legal framework providing for a regulation of Medical Devices? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	There is no specific legal framework.
Case-law:	-
Other:	-

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
eHealth and mHealth:	Does the concept of Medical device in your country encompass services and apparels in the realm of eHealth and mHealth? What are the requirements? Should, for instance, the medical device be certified before it can be used?
	Not to our knowledge.
Apps:	Does the concept of medical devices encompass apps? If yes, is there any regulation applicable to apps that perform medical services? Is there any regulation applicable on apps that track non-medical data that can lead to health information? If yes, what type of data?
	Not to our knowledge.
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical and/or wearable devices? If yes, what are the standards?
	No formal requirement.
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical treatment? How would this be applied to fitness and daily-basis data?
	Not to our knowledge.

6. Internet of Things

6.1. Data Protection Issues:

Internet of things relates to common, ordinary devices that are now, and increasingly, connected to the Internet, such as cars, fridges, ovens, microwaves, etc. All of these devices can provide data that can lead to reveal information concerning one's health. A fridge can easily inform on the type of food stored and thus the diet of an individual. One of the biggest challenges of the Internet of Things is to guarantee the right to privacy and data protection in a world where every device collects, processes, analyses and transmits the data, commonly via wireless technologies.

In the realm of medical data, the issue mainly arises when crossing seemly unrelated data that can lead to health information about an individual.

6.2. Questions: Is your legal framework providing for a regulation of the Internet of Things? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	Internet of Things as such is not regulated in our legislation.
Case-law:	

Other:	Information Commissioner has issued some opinions that would fall under the realm of Internet of Things, such as the opinions on e-toll collection (https://www.ip-rs.si/fileadmin/user_upload/Pdf/razno/Opinion_on_electronic_toll_collection_Information_Commissioner_Slovenia.pdf), intelligent video analytics and smart grids.

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Security:	What are the security standards that need to be employed by these devices when collecting personal data?
	General data protection rules (PDPA) would apply for data controllers from our country that would process personal data collected through the use of different devices. The most important aspects would be the main principles - who is the data controller, which data are collected and on which legal ground, for which purposes etc. and what is the adequate level of security measures.
Non-medical devices:	Are non-medical devices allowed to collect medical data, such as heart frequency? Are they allowed to cross medical data with non-medical data?
	General data protection rules (PDPA) would apply, as above. There is no specific provision that would regulate this.
Privacy by Design:	Is there any requirement to implement privacy by design in the development of connected devices? If yes, what are the standards?
	There is no such formal requirement in the legal frameworks. Information Commissioner has issued guidelines on development of information solutions that promote the privacy by design approach: https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice_za_razvoj_informacijski_resitev_ENG.pdf

7. Electronic Doctor (online Doctor) and on-line appointments

7.1. Data Protection Issues:

The Doctor listens, talks and assesses the patient online, via a website, app, canal, sometimes including video-conference. Medical data is collected and processed, what are the security requirements and standards followed? Other websites provide for on-line appointments with doctors, which can also involve the processing of medical data.

7.2. Questions: Is your legal framework providing for a regulation of online Medical Treatment and is the on-line appointment system covered by such a framework? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	There is no specific legal framework.
Case-law:	-
Other:	-

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Medical treatment:	Is it allowed to perform medical treatment via online services? If yes, how should the medical services be provided? Does it have to follow the same requirements of a regular physically-present medical treatment?

	There are no specific restrictions to perform medical treatment via online services? General rule must be followed: "*In the transmission of sensitive personal data over telecommunications networks, data shall be considered as suitably protected if they are sent with the use of cryptographic methods and electronic signatures such that their illegibility or non-recognition is ensured during transmission*".
Medical data:	How should the data collected via a medical treatment performed online be processed? Are there specific requirements? Which ones?
	See above.

Other comments and technologies
Should you wish to describe any technology, feature or trend that has not been covered by the questionnaire, please feel free to use the space provided below. Where relevant, also indicate recent legislation changes, guidelines and/or case law.
We would like to point out that the deployment of some modern technologies is lagging behind due to various and complex reasons; therefore many of the issues raised in the questionnaire cannot be addresses more precisely and legislation has thus far not been adopted that would regulated some of the highlighted issues. General data protection rules, as stipulated in the PDPA, would therefore apply. There may be significant differences from case to case as regards all the aspects of data protection (e.g. there may be several possible legal grounds, different data controllers and different purposes) therefore is not possible to list them all or summarize them. We presume that more specific answers and examples could be provided by health policy authorities, professional or patient associations as well as healthcare providers.

THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA" / «L'EX-REPUBLIQUE YOUGOSLAVE DE MACEDOINE»

PUBLIC HEALTH CARE 1.

QUESTIONNAIRE

The questionnaire should ideally be completed by data protection authorities, health policy authorities, professional or patient associations as well as healthcare providers: you are invited to share it as widely as possible.

Please send your replies to dataprotection@coe.int no later than 15 December 2014.

1. Mobile Health (mHealth) and Electronic Health Records (EHR)

1.1. Data Protection Issues:
This is perhaps the biggest topic sitting at the intersection of technology and data protection. Mobile health (mHealth) and Electronic Health Records (EHR) are increasingly used in healthcare systems and provisions – it is a trend that needs to be examined. Related to the EHR, these records are more accurate, cost-effective (in terms of storage) than paper-based notes. The concept of patient controlled/accessed EHR has been implemented in varying degrees in different countries. Furthermore, some non-medical record can still contain health information about users and it should be considered if such records ought to be treated in a similar way to EHR. Also, should 'medical data' as defined in Recommendation N° (97) 5 on the protection of medical data cover physical tracking data, such as pedometers or fitness data and data that can lead to medical information about an individual ?

1.2. Questions: if EHR exist in your country, is your legal framework providing for a regulation of such records? If mHealth exists in your country, is your legal framework providing for a specific regulation? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	Yes, in accordance with the Rulebook for e-medical records given br thye Ministry of health.
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
EHR and Medical data:	What can be considered medical data in your country? Is it solely the data relating to a person's health (state, diagnosis, prognosis, medical treatment, etc.)? Is non-medical data that leads to medical information treated the same way as medical data (for instance in terms of confidentiality requirements)? Is the EHR solely constituted of data collected in a medical context or can the individual also himself or herself add information regarding his or her health?
	The individual cannot add info by himself, but this info is collected by third parties.
Sharing of data and Access:	Who is granted access to the EHR and how is the sharing of information (with other health care providers?) regulated? Where information is shared with

	pharmacists, is there a strict purpose limitation in place? How has the definition of the responsibility over the medical data been regulated?
	Yes, limited access in accordance to the level of access
Data quality:	Are the principles of legitimacy, fairness and minimization applied to medical data? How are records kept accurate? How long is the data kept for, is the specific storage period defined for the EHR?
	Yes, the principle of minimization is used and there are due dates.
Data integrity:	Are any specific methods used to ensure the integrity of the data? How are patients identified in the EHR? In the context of research, are anonymisation methods used and what safeguards exist for re-identification?
	Yes, with multi-level of security, varying from physical to electronic safety (anti-viruses, firewalls..)
Data security:	Where are the records stored? Is there a centralized database of EHR? What security technology is being used?
	Centralized data base with multi-level security.
Rights of the person/patient concerned:	How can the right of access be exercised? How can the data be corrected? Can the person enter information in his or her own EHR? What are the legal remedies available?
	Only on personal request by the patient as well as the court for the purpose of investigation.
Consent:	Is the system based on an opt-in approach? Is the principle of granular consent applied (with the possibility of preventing access to certain data?)? If yes, in which situations?
	Yes there is a limit on request of the patient with the order of a superior person.
Withdrawal:	Are patients able to withdraw the consent given to EHR schemes? If yes, what is the relevant procedure to withdraw such consent? What are the consequences?
	It is not permitted because this way of recording is implemented in the health system and will have huge consequences in further treatment of the patient.
Outsourcing processing of data:	Is outsourcing common? Under what circumstances? Where is the data outsourced to? What sort of safeguards are in place?
	It is possible. The records should be kept in the programming houses on special server or expert HDD that previously signed an agreement.

2. Cloud Computing, Data Mining and Profiling from both Medical Records (including EHR) and Data not specifically related to medical records.

2.1. Data Protection Issues:

Cloud computing has brought a new dimension to the way data is stored, accessed and processed. Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS), Network as a service (NaaS) are all used by services and organisations that deal with both medical data and non-medical data.

With the development of more advanced and efficient data-mining and data-querying Medical

techniques (e.g NoSQL, MapReduce, Hadoop) in conjunction with increased processing power and data storage, mining data has never been more informative, easier, and cost-effective.

Healthcare is a natural sector in which to apply new technologies and methodologies, with particular impacts in epidemiology, public health, health services research, etc.

Data that can lead to the identification of a particular individual and his/her health situation is not limited to medical data *per se,* present on Electronic Health Records, but also to unsuspicious type of information.

There is a growing concern that these schemes may be implemented in manner which does not always respect the patients' confidentiality and basic rights, and in a broader context, the use of this of information may prejudice the individuals concerned.

The ability to track and monitor patients and resources enables a more efficient provision of care but may have an impact on the right to privacy of the individual concerned.

2.2. Questions: Is your legal framework providing for a regulation of Cloud Computing, Data Mining and Profiling? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Cloud computing:	How is cloud computing regulated in your country? Which security safeguards and standards are mandatory? Are there specific requirements in order to store medical data in the cloud? How is data shared and is the sharing regulated?
Government:	Do governmental programmes exist to allow for increased data-mining of medical records? If yes, what are the purposes of this data mining? Are private entities allowed to access the data? Under what circumstances? What sort of techniques and technologies are being used? To what end? Are data subjects informed of this type of data-mining?
Private sector:	Are private entities allowed to mine medical data which they process? Under what circumstances? Can the government have access to this data?
Profiling:	Are the government and the private sector allowed to employ profiling methods on medical data? If yes, under what circumstances? Is it allowed to cross and correlate non-medical data with medical data?

3. RFID and wireless communication technologies

3.1. Data Protection Issues:

It is common for medical devices, such as patients' tags, to possess RFID technologies in order to facilitate the transmission of the patients' data.

It can also be related to the data-mining operations previously mentioned as it is another category of information that can be used to discern meaningful patterns.

Transmission of data through radio-frequency is not limited to medical devices. Almost any smartphone uses some technology enabling to collect, and share, the user's data. For instance, via WI-FI it is possible to identify users' locations and therefore infer some of their behaviour, which in some cases can relate to health information.

3.2. Questions: Is your legal framework providing for a regulation of RFID technologies and the transfer of personal data through wireless technologies? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
RFID:	How is RFID used in hospital/clinics for (a) resource management, (b) patient care? What types of database systems (and security) are implemented in conjunction with RFID use? How are issues of access, sharing, consent etc. managed considering that RFID may be used without the patients' knowledge.
	NO
Wireless tracking technologies:	Are hospitals/clinics employing other wireless tracking technologies besides RFID? Which ones? Do they have to follow specific security requirements? Which ones?
	NO

4. Applications (Mobile)

4.1. Data Protection Issues:
Information society is increasingly relying on the use of "apps" (application), most of them mobile. These apps are commonly designed to gather personal data, and in practice often process medical data. Technologies such as multi-touch touchscreen, accelerometers or gyroscopes, ambient light sensors, GPS and cameras, and devices featuring fingerprint and biometric sensors also involve the collection of medical data. A mobile phone application can monitor accurately physiological data, such as heartbeats, sleep patterns, fitness information.

4.2. Questions: Is your legal framework providing for a regulation of Apps and Mobile Apps? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Apps:	Is it allowed to use apps and mobile apps to deploy medical services and collect medical data? If yes, which type of individual/organisation can develop and employ these apps? Are there specific security requirements for these types of apps?

	Yes, but only doctors within the sector they work in.
Institutions:	Do hospitals/clinics/labs employ apps to gather medical data? Is there a need for a medical treatment to permit the use of an app to process the medical data? Are there specific security requirements for the institutions collecting these data from the apps? Are medico-administrative data used by hospitals/clinics for management purposes?
Tracking technologies:	Do hospitals/clinics/labs employ non-medical apps and devices to track and collect data from their patients? What type of data is collected? For what purpose? Is the data identifiable? Is the data combined with medical data?
	There is no such a technology.
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical apps and tracking apps? If yes, what are the standards?
	There are no such requests
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical diagnostic? How would this be applied to fitness and daily-basis data?

5. Medical Devices and Wearable Devices

5.1. Data Protection Issues:

A medical device can be defined as: 'any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application. Such a device should be intended by the manufacturer for one of a number of defined purposes, one of which is, diagnosis, prevention, monitoring, treatment or alleviation of disease' (Directive 93/42/EEC Article 1:2)

Some eHealth and mHealth devices and apps do not fall in this definition of medical devices, as can also be the case of a software working in combination with a physical device, for instance a smartphone.

5.2. Questions: Is your legal framework providing for a regulation of Medical Devices? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
eHealth and mHealth:	Does the concept of Medical device in your country encompass services and apparels in the realm of eHealth and mHealth? What are the requirements? Should, for instance, the medical device be certified before it can be used?
	Yes, only certified devices.

Apps:	Does the concept of medical devices encompass apps? If yes, is there any regulation applicable to apps that perform medical services? Is there any regulation applicable on apps that track non-medical data that can lead to health information? If yes, what type of data?
	Yes, under the jurisdiction of Ministry of health.
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical and/or wearable devices? If yes, what are the standards?
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical treatment? How would this be applied to fitness and daily-basis data?

6. Internet of Things

6.1. Data Protection Issues:

Internet of things relates to common, ordinary devices that are now, and increasingly, connected to the Internet, such as cars, fridges, ovens, microwaves, etc. All of these devices can provide data that can lead to reveal information concerning one's health. A fridge can easily inform on the type of food stored and thus the diet of an individual. One of the biggest challenges of the Internet of Things is to guarantee the right to privacy and data protection in a world where every device collects, processes, analyses and transmits the data, commonly via wireless technologies.

In the realm of medical data, the issue mainly arises when crossing seemly unrelated data that can lead to health information about an individual.

6.2. Questions: Is your legal framework providing for a regulation of the Internet of Things? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Security:	What are the security standards that need to be employed by these devices when collecting personal data?
Non-medical devices:	Are non-medical devices allowed to collect medical data, such as heart frequency? Are they allowed to cross medical data with non-medical data?
	NO
Privacy by Design:	Is there any requirement to implement privacy by design in the development of connected devices? If yes, what are the standards?

7. Electronic Doctor (online Doctor) and on-line appointments

7.1. Data Protection Issues:
The Doctor listens, talks and assesses the patient online, via a website, app, canal, sometimes including video-conference. Medical data is collected and processed, what are the security requirements and standards followed? Other websites provide for on-line appointments with doctors, which can also involve the processing of medical data.

7.2. Questions: Is your legal framework providing for a regulation of online Medical Treatment and is the on-line appointment system covered by such a framework? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Medical treatment:	Is it allowed to perform medical treatment via online services? If yes, how should the medical services be provided? Does it have to follow the same requirements of a regular physically-present medical treatment?
	It is not allowed.
Medical data:	How should the data collected via a medical treatment performed online be processed? Are there specific requirements? Which ones?

Other comments and technologies
Should you wish to describe any technology, feature or trend that has not been covered by the questionnaire, please feel free to use the space provided below. Where relevant, also indicate recent legislation changes, guidelines and/or case law.

PUBLIC HEALTH CARE 2.

QUESTIONNAIRE

The questionnaire should ideally be completed by data protection authorities, health policy authorities, professional or patient associations as well as healthcare providers: you are invited to share it as widely as possible.

Please send your replies to dataprotection@coe.int no later than 15 December 2014.

1. Mobile Health (mHealth) and Electronic Health Records (EHR)

1.1. Data Protection Issues:

This is perhaps the biggest topic sitting at the intersection of technology and data protection. Mobile health (mHealth) and Electronic Health Records (EHR) are increasingly used in healthcare systems and provisions – it is a trend that needs to be examined.

Related to the EHR, these records are more accurate, cost-effective (in terms of storage) than paper-based notes. The concept of patient controlled/accessed EHR has been implemented in varying degrees in different countries.

Furthermore, some non-medical record can still contain health information about users and it should be considered if such records ought to be treated in a similar way to EHR.

Also, should 'medical data' as defined in Recommendation N° (97) 5 on the protection of medical data cover physical tracking data, such as pedometers or fitness data and data that can lead to medical information about an individual ?

1.2. Questions: if EHR exist in your country, is your legal framework providing for a regulation of such records? If mHealth exists in your country, is your legal framework providing for a specific regulation? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	Yes, in accordance with the Rulebook for e-medical records given br thye Ministry of health.
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
EHR and Medical data:	What can be considered medical data in your country? Is it solely the data relating to a person's health (state, diagnosis, prognosis, medical treatment, etc.)? Is non-medical data that leads to medical information treated the same way as medical data (for instance in terms of confidentiality requirements)? Is the EHR solely constituted of data collected in a medical context or can the individual also himself or herself add information regarding his or her health?
	The individual cannot add info by himself, but this info is collected by third parties.
Sharing of data and Access:	Who is granted access to the EHR and how is the sharing of information (with other health care providers?) regulated? Where information is shared with pharmacists, is there a strict purpose limitation in place? How has the definition of the responsibility over the medical data been regulated?

	Yes, limited access in accordance to the level of access.
Data quality:	Are the principles of legitimacy, fairness and minimization applied to medical data? How are records kept accurate? How long is the data kept for, is the specific storage period defined for the EHR?
	Yes, the principle of minimization is used and there are due dates.
Data integrity:	Are any specific methods used to ensure the integrity of the data? How are patients identified in the EHR? In the context of research, are anonymisation methods used and what safeguards exist for re-identification?
	Yes, with multi-level of security, varying from physical to electronic safety (anti-viruses, firewalls..)
Data security:	Where are the records stored? Is there a centralized database of EHR? What security technology is being used?
	Centralized data base with multi-level security.
Rights of the person/patient concerned:	How can the right of access be exercised? How can the data be corrected? Can the person enter information in his or her own EHR? What are the legal remedies available?
	Only on personal request by the patient as well as the court for the purpose of investigation.
Consent:	Is the system based on an opt-in approach? Is the principle of granular consent applied (with the possibility of preventing access to certain data?)? If yes, in which situations?
	Yes there is a limit on request of the patient with the order of a superior person.
Withdrawal:	Are patients able to withdraw the consent given to EHR schemes? If yes, what is the relevant procedure to withdraw such consent? What are the consequences?
	It is not permitted because this way of recording is implemented in the health system and will have huge consequences in further treatment of the patient.
Outsourcing processing of data:	Is outsourcing common? Under what circumstances? Where is the data outsourced to? What sort of safeguards are in place?
	It is possible. The records should be kept in the programming houses on special server or expert HDD that previously signed an agreement.

2. Cloud Computing, Data Mining and Profiling from both Medical Records (including EHR) and Data not specifically related to medical records.

2.1. Data Protection Issues:

Cloud computing has brought a new dimension to the way data is stored, accessed and processed. Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS), Network as a service (NaaS) are all used by services and organisations that deal with both medical data and non-medical data.

With the development of more advanced and efficient data-mining and data-querying Medical techniques (e.g NoSQL, MapReduce, Hadoop) in conjunction with increased processing power and data storage, mining data has never been more informative, easier, and cost-effective.

Healthcare is a natural sector in which to apply new technologies and methodologies, with particular impacts in epidemiology, public health, health services research, etc.

Data that can lead to the identification of a particular individual and his/her health situation is not limited to medical data *per se,* present on Electronic Health Records, but also to unsuspicious type of information.

There is a growing concern that these schemes may be implemented in manner which does not always respect the patients' confidentiality and basic rights, and in a broader context, the use of this of information may prejudice the individuals concerned.

The ability to track and monitor patients and resources enables a more efficient provision of care but may have an impact on the right to privacy of the individual concerned.

2.2. Questions: Is your legal framework providing for a regulation of Cloud Computing, Data Mining and Profiling? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Cloud computing:	How is cloud computing regulated in your country? Which security safeguards and standards are mandatory? Are there specific requirements in order to store medical data in the cloud? How is data shared and is the sharing regulated?
Government:	Do governmental programmes exist to allow for increased data-mining of medical records? If yes, what are the purposes of this data mining? Are private entities allowed to access the data? Under what circumstances? What sort of techniques and technologies are being used? To what end? Are data subjects informed of this type of data-mining?
Private sector:	Are private entities allowed to mine medical data which they process? Under what circumstances? Can the government have access to this data?
Profiling:	Are the government and the private sector allowed to employ profiling methods on medical data? If yes, under what circumstances? Is it allowed to cross and correlate non-medical data with medical data?

3. RFID and wireless communication technologies

3.1. Data Protection Issues:

It is common for medical devices, such as patients' tags, to possess RFID technologies in order to facilitate the transmission of the patients' data.

It can also be related to the data-mining operations previously mentioned as it is another category of information that can be used to discern meaningful patterns.

Transmission of data through radio-frequency is not limited to medical devices. Almost any smartphone uses some technology enabling to collect, and share, the user's data. For instance, via WI-FI it is possible to identify users' locations and therefore infer some of their behaviour, which in some cases can relate to health information.

3.2. Questions: Is your legal framework providing for a regulation of RFID technologies and the transfer of personal data through wireless technologies? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
RFID:	How is RFID used in hospital/clinics for (a) resource management, (b) patient care? What types of database systems (and security) are implemented in conjunction with RFID use? How are issues of access, sharing, consent etc. managed considering that RFID may be used without the patients' knowledge.
	NO
Wireless tracking technologies:	Are hospitals/clinics employing other wireless tracking technologies besides RFID? Which ones? Do they have to follow specific security requirements? Which ones?
	NO

4. Applications (Mobile)

4.1. Data Protection Issues:

Information society is increasingly relying on the use of "apps" (application), most of them mobile. These apps are commonly designed to gather personal data, and in practice often process medical data.
Technologies such as multi-touch touchscreen, accelerometers or gyroscopes, ambient light sensors, GPS and cameras, and devices featuring fingerprint and biometric sensors also involve the collection of medical data.

A mobile phone application can monitor accurately physiological data, such as heartbeats, sleep patterns, fitness information.

4.2. Questions: Is your legal framework providing for a regulation of Apps and Mobile Apps? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Apps:	Is it allowed to use apps and mobile apps to deploy medical services and collect medical data? If yes, which type of individual/organisation can develop and employ these apps? Are there specific security requirements for these types of apps?
	Yes, but only doctors within the sector they work in.
Institutions:	Do hospitals/clinics/labs employ apps to gather medical data? Is there a need for a medical treatment to permit the use of an app to process the medical data? Are there specific security requirements for the institutions collecting these data from the apps? Are medico-administrative data used by hospitals/clinics for management purposes?
Tracking technologies:	Do hospitals/clinics/labs employ non-medical apps and devices to track and collect data from their patients? What type of data is collected? For what purpose? Is the data identifiable? Is the data combined with medical data?
	There is no such a technology.
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical apps and tracking apps? If yes, what are the standards?
	There are no such requests
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical diagnostic? How would this be applied to fitness and daily-basis data?

5. Medical Devices and Wearable Devices

5.1. Data Protection Issues:

A medical device can be defined as: 'any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application. Such a device should be intended by the manufacturer for one of a number of defined purposes, one of which is, diagnosis, prevention, monitoring, treatment or alleviation of disease' (Directive 93/42/EEC Article 1:2)

Some eHealth and mHealth devices and apps do not fall in this definition of medical devices, as can also be the case of a software working in combination with a physical device, for instance a smartphone.

5.2. Questions: Is your legal framework providing for a regulation of Medical Devices? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
eHealth and mHealth:	Does the concept of Medical device in your country encompass services and apparels in the realm of eHealth and mHealth? What are the requirements? Should, for instance, the medical device be certified before it can be used?
	Yes, only certified devices.
Apps:	Does the concept of medical devices encompass apps? If yes, is there any regulation applicable to apps that perform medical services? Is there any regulation applicable on apps that track non-medical data that can lead to health information? If yes, what type of data?
	Yes, under the jurisdiction of Ministry of health.
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical and/or wearable devices? If yes, what are the standards?
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical treatment? How would this be applied to fitness and daily-basis data?

6. Internet of Things

6.1. Data Protection Issues:

Internet of things relates to common, ordinary devices that are now, and increasingly, connected to the Internet, such as cars, fridges, ovens, microwaves, etc. All of these devices can provide data that can lead to reveal information concerning one's health. A fridge can easily inform on the type of food stored and thus the diet of an individual. One of the biggest challenges of the Internet of Things is to guarantee the right to privacy and data protection in a world where every device collects, processes, analyses and transmits the data, commonly via wireless technologies.

In the realm of medical data, the issue mainly arises when crossing seemly unrelated data that can lead to health information about an individual.

6.2. Questions: Is your legal framework providing for a regulation of the Internet of Things? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Security:	What are the security standards that need to be employed by these devices when collecting personal data?
Non-medical devices:	Are non-medical devices allowed to collect medical data, such as heart frequency? Are they allowed to cross medical data with non-medical data?

	NO
Privacy by Design:	Is there any requirement to implement privacy by design in the development of connected devices? If yes, what are the standards?

7. Electronic Doctor (online Doctor) and on-line appointments

7.1. Data Protection Issues:

The Doctor listens, talks and assesses the patient online, via a website, app, canal, sometimes including video-conference. Medical data is collected and processed, what are the security requirements and standards followed? Other websites provide for on-line appointments with doctors, which can also involve the processing of medical data.

7.2. Questions: Is your legal framework providing for a regulation of online Medical Treatment and is the on-line appointment system covered by such a framework? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Medical treatment:	Is it allowed to perform medical treatment via online services? If yes, how should the medical services be provided? Does it have to follow the same requirements of a regular physically-present medical treatment?
	It is not allowed.
Medical data:	How should the data collected via a medical treatment performed online be processed? Are there specific requirements? Which ones?

Other comments and technologies
Should you wish to describe any technology, feature or trend that has not been covered by the questionnaire, please feel free to use the space provided below. Where relevant, also indicate recent legislation changes, guidelines and/or case law.

PRIVATE HEALTH CARE 3.

QUESTIONNAIRE

The questionnaire should ideally be completed by data protection authorities, health policy authorities, professional or patient associations as well as healthcare providers: you are invited to share it as widely as possible.

Please send your replies to dataprotection@coe.int no later than 15 December 2014.

1. Mobile Health (mHealth) and Electronic Health Records (EHR)

1.1. Data Protection Issues:

This is perhaps the biggest topic sitting at the intersection of technology and data protection. Mobile health (mHealth) and Electronic Health Records (EHR) are increasingly used in healthcare systems and provisions – it is a trend that needs to be examined.

Related to the EHR, these records are more accurate, cost-effective (in terms of storage) than paper-based notes. The concept of patient controlled/accessed EHR has been implemented in varying degrees in different countries.

Furthermore, some non-medical record can still contain health information about users and it should be considered if such records ought to be treated in a similar way to EHR.

Also, should 'medical data' as defined in Recommendation N° (97) 5 on the protection of medical data cover physical tracking data, such as pedometers or fitness data and data that can lead to medical information about an individual ?

1.2. Questions: if EHR exist in your country, is your legal framework providing for a regulation of such records? If mHealth exists in your country, is your legal framework providing for a specific regulation? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
EHR and Medical data:	What can be considered medical data in your country? Is it solely the data relating to a person's health (state, diagnosis, prognosis, medical treatment, etc.)? Is non-medical data that leads to medical information treated the same way as medical data (for instance in terms of confidentiality requirements)? Is the EHR solely constituted of data collected in a medical context or can the individual also himself or herself add information regarding his or her health?
	Alongside all the medical data here is also included the not-so-medical data (height, weight, gender, unique number of insured health, health card number, address, education, etc.). All the date of the individual is treaded the same way when it comes to confidentiality. The individual cannot add or change himself any data regarding his health condition.
Sharing of data and Access:	Who is granted access to the EHR and how is the sharing of information (with other health care providers?) regulated? Where information is shared with pharmacists, is there a strict purpose limitation in place? How has the definition of the responsibility over the medical data been regulated?

	Suitable institutions and individuals with pre-defined protocols and media (my appointment, web side), consistent with the law in the attention about the protection of personal data
Data quality:	Are the principles of legitimacy, fairness and minimisation applied to medical data? How are records kept accurate? How long is the data kept for, is the specific storage period defined for the EHR?
	Yes, there are applied. There is.
Data integrity:	Are any specific methods used to ensure the integrity of the data? How are patients identified in the EHR? In the context of research, are anonymisation methods used and what safeguards exist for re-identification?
	It is applied an electronic health card with a corresponding chip and pin code for identification. Unique number of insured health, unique identification number
Data security:	Where are the records stored? Is there a centralised database of EHR? What security technology is being used?
	There is central database (my appointment) – security measures – Ministry of Health
Rights of the person/patient concerned:	How can the right of access be exercised? How can the data be corrected? Can the person enter information in his or her own EHR? What are the legal remedies available?
	According to the law on protection of personal data the patient has the right to inspect their data, as well as correction and insight into security-protection of personal data
Consent:	Is the system based on an opt-in approach? Is the principle of granular consent applied (with the possibility of preventing access to certain data?)? If yes, in which situations?
	/
Withdrawal:	Are patients able to withdraw the consent given to EHR schemes? If yes, what is the relevant procedure to withdraw such consent? What are the consequences?
	No indications
Outsourcing processing of data:	Is outsourcing common? Under what circumstances? Where is the data outsourced to? What sort of safeguards are in place?
	Unknown

2. Cloud Computing, Data Mining and Profiling from both Medical Records (including EHR) and Data not specifically related to medical records.

2.1. Data Protection Issues:

Cloud computing has brought a new dimension to the way data is stored, accessed and processed. Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS), Network as a service (NaaS) are all used by services and organisations that deal with both medical data and non-medical data.

With the development of more advanced and efficient data-mining and data-querying Medical techniques (e.g NoSQL, MapReduce, Hadoop) in conjunction with increased processing power and data storage, mining data has never been more informative, easier, and cost-effective.

Healthcare is a natural sector in which to apply new technologies and methodologies, with particular impacts in epidemiology, public health, health services research, etc.

Data that can lead to the identification of a particular individual and his/her health situation is not limited to medical data *per se,* present on Electronic Health Records, but also to unsuspicious type of information.

There is a growing concern that these schemes may be implemented in manner which does not always respect the patients' confidentiality and basic rights, and in a broader context, the use of this of information may prejudice the individuals concerned.

The ability to track and monitor patients and resources enables a more efficient provision of care but may have an impact on the right to privacy of the individual concerned.

2.2. Questions: Is your legal framework providing for a regulation of Cloud Computing, Data Mining and Profiling? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	Law on Personal Data Protection
Case-law:	/
Other:	/

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Cloud computing:	How is cloud computing regulated in your country? Which security safeguards and standards are mandatory? Are there specific requirements in order to store medical data in the cloud? How is data shared and is the sharing regulated?
	Unknown
Government:	Do governmental programmes exist to allow for increased data-mining of medical records? If yes, what are the purposes of this data mining? Are private entities allowed to access the data? Under what circumstances? What sort of techniques and technologies are being used? To what end? Are data subjects informed of this type of data-mining?
	Unknown
Private sector:	Are private entities allowed to mine medical data which they process? Under what circumstances? Can the government have access to this data?
	Unknown
Profiling:	Are the government and the private sector allowed to employ profiling methods on medical data? If yes, under what circumstances? Is it allowed to cross and correlate non-medical data with medical data?
	Unknown

3. RFID and wireless communication technologies

3.1. Data Protection Issues:

It is common for medical devices, such as patients' tags, to possess RFID technologies in order to facilitate the transmission of the patients' data.

It can also be related to the data-mining operations previously mentioned as it is another category of information that can be used to discern meaningful patterns.

Transmission of data through radio-frequency is not limited to medical devices. Almost any smartphone uses some technology enabling to collect, and share, the user's data. For instance, via WI-FI it is possible to identify users' locations and therefore infer some of their behaviour, which in some cases can relate to health information.

3.2. Questions: Is your legal framework providing for a regulation of RFID technologies and the transfer of personal data through wireless technologies? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	Unknown
Case-law:	/
Other:	/

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
RFID:	How is RFID used in hospital/clinics for (a) resource management, (b) patient care? What types of database systems (and security) are implemented in conjunction with RFID use? How are issues of access, sharing, consent etc. managed considering that RFID may be used without the patients' knowledge.
	Unknown
Wireless tracking technologies:	Are hospitals/clinics employing other wireless tracking technologies besides RFID? Which ones? Do they have to follow specific security requirements? Which ones?
	Unknown

4. Applications (Mobile)

4.1. Data Protection Issues:

Information society is increasingly relying on the use of "apps" (application), most of them mobile. These apps are commonly designed to gather personal data, and in practice often process medical data.
Technologies such as multi-touch touchscreen, accelerometers or gyroscopes, ambient light sensors, GPS and cameras, and devices featuring fingerprint and biometric sensors also involve the collection of medical data.

A mobile phone application can monitor accurately physiological data, such as heartbeats, sleep patterns, fitness information.

4.2. Questions: Is your legal framework providing for a regulation of Apps and Mobile Apps? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	Unknown
Case-law:	Unknown
Other:	Unknown
Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Apps:	Is it allowed to use apps and mobile apps to deploy medical services and collect medical data? If yes, which type of individual/organisation can develop and employ these apps? Are there specific security requirements for these types of apps?
	No
Institutions:	Do hospitals/clinics/labs employ apps to gather medical data? Is there a need for a medical treatment to permit the use of an app to process the medical data? Are there specific security requirements for the institutions collecting these data from the apps? Are medico-administrative data used by hospitals/clinics for management purposes?
	Unknown
Tracking technologies:	Do hospitals/clinics/labs employ non-medical apps and devices to track and collect data from their patients? What type of data is collected? For what purpose? Is the data identifiable? Is the data combined with medical data?
	Unknown
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical apps and tracking apps? If yes, what are the standards?
	Unknown
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical diagnostic? How would this be applied to fitness and daily-basis data?
	Unknown

5. Medical Devices and Wearable Devices

5.1. Data Protection Issues:

A medical device can be defined as: 'any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application. Such a device should be intended by the manufacturer for one of a number of defined purposes, one of which is, diagnosis, prevention, monitoring, treatment or alleviation of disease' (Directive 93/42/EEC Article 1:2)

Some eHealth and mHealth devices and apps do not fall in this definition of medical devices, as can also be the case of a software working in combination with a physical device, for instance a smartphone.

5.2. Questions: Is your legal framework providing for a regulation of Medical Devices? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	Unknown
Case-law:	/
Other:	/

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
eHealth and mHealth:	Does the concept of Medical device in your country encompass services and apparels in the realm of eHealth and mHealth? What are the requirements? Should, for instance, the medical device be certified before it can be used?
	Unknown
Apps:	Does the concept of medical devices encompass apps? If yes, is there any regulation applicable to apps that perform medical services? Is there any regulation applicable on apps that track non-medical data that can lead to health information? If yes, what type of data?
	Yes
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical and/or wearable devices? If yes, what are the standards?
	Unknown
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical treatment? How would this be applied to fitness and daily-basis data?
	Unknown

6. Internet of Things

6.1. Data Protection Issues:

Internet of things relates to common, ordinary devices that are now, and increasingly, connected to the Internet, such as cars, fridges, ovens, microwaves, etc. All of these devices can provide data that can lead to reveal information concerning one's health. A fridge can easily inform on the type of food stored and thus the diet of an individual. One of the biggest challenges of the Internet of Things is to guarantee the right to privacy and data protection in a world where every device collects, processes, analyses and transmits the data, commonly via wireless technologies.

In the realm of medical data, the issue mainly arises when crossing seemly unrelated data that can lead to health information about an individual.

6.2. Questions: Is your legal framework providing for a regulation of the Internet of Things? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	Unknown
Case-law:	Unknown
Other:	Unknown

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Security:	What are the security standards that need to be employed by these devices when collecting personal data?
	Unknown
Non-medical devices:	Are non-medical devices allowed to collect medical data, such as heart frequency? Are they allowed to cross medical data with non-medical data?
	Unknown
Privacy by Design:	Is there any requirement to implement privacy by design in the development of connected devices? If yes, what are the standards?
	Unknown

7. Electronic Doctor (online Doctor) and on-line appointments

7.1. Data Protection Issues:

The Doctor listens, talks and assesses the patient online, via a website, app, canal, sometimes including video-conference. Medical data is collected and processed, what are the security requirements and standards followed? Other websites provide for on-line appointments with doctors, which can also involve the processing of medical data.

7.2. Questions: Is your legal framework providing for a regulation of online Medical Treatment and is the on-line appointment system covered by such a framework? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	Unknown
Case-law:	Unknown
Other:	Unknown

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Medical treatment:	Is it allowed to perform medical treatment via online services? If yes, how should the medical services be provided? Does it have to follow the same requirements of a regular physically-present medical treatment?
	Unknown
Medical data:	How should the data collected via a medical treatment performed online be processed? Are there specific requirements? Which ones?
	Unknown

Other comments and technologies
Should you wish to describe any technology, feature or trend that has not been covered by the questionnaire, please feel free to use the space provided below. Where relevant, also indicate recent legislation changes, guidelines and/or case law.
/

PRIVATE HEALTH CARE 4.

QUESTIONNAIRE

The questionnaire should ideally be completed by data protection authorities, health policy authorities, professional or patient associations as well as healthcare providers: you are invited to share it as widely as possible.

Please send your replies to dataprotection@coe.int no later than 15 December 2014.

1. Mobile Health (mHealth) and Electronic Health Records (EHR)

1.1. Data Protection Issues:

This is perhaps the biggest topic sitting at the intersection of technology and data protection. Mobile health (mHealth) and Electronic Health Records (EHR) are increasingly used in healthcare systems and provisions – it is a trend that needs to be examined.

Related to the EHR, these records are more accurate, cost-effective (in terms of storage) than paper-based notes. The concept of patient controlled/accessed EHR has been implemented in varying degrees in different countries.

Furthermore, some non-medical record can still contain health information about users and it should be considered if such records ought to be treated in a similar way to EHR.

Also, should 'medical data' as defined in Recommendation N° (97) 5 on the protection of medical data cover physical tracking data, such as pedometers or fitness data and data that can lead to medical information about an individual ?

1.2. Questions: if EHR exist in your country, is your legal framework providing for a regulation of such records? If mHealth exists in your country, is your legal framework providing for a specific regulation? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
EHR and Medical data:	What can be considered medical data in your country? Is it solely the data relating to a person's health (state, diagnosis, prognosis, medical treatment, etc.)? Is non-medical data that leads to medical information treated the same way as medical data (for instance in terms of confidentiality requirements)? Is the EHR solely constituted of data collected in a medical context or can the individual also himself or herself add information regarding his or her health?
	Medical data means the data related to the health condition of the patients, but the legislation recognizes other delicate personal data (related to genetics, sexuality, etc.) for which the legislation sets the highest bar of confidentiality The individual cannot add data related to him medical condition himself.
Sharing of data and Access:	Who is granted access to the EHR and how is the sharing of information (with other health care providers?) regulated? Where information is shared with pharmacists, is there a strict purpose limitation in place? How has the definition of

	the responsibility over the medical data been regulated?
	Access to the EHR have only medical workers that work within the FZOM and the health authorities (FZOM and Ministry of health authorization and access level to check with them.
Data quality:	Are the principles of legitimacy, fairness and minimisation applied to medical data? How are records kept accurate? How long is the data kept for, is the specific storage period defined for the EHR?
	Under the Law on records in the field of health (15 years after the last entry in EHR)
Data integrity:	Are any specific methods used to ensure the integrity of the data? How are patients identified in the EHR? In the context of research, are anonymisation methods used and what safeguards exist for re-identification?
Data security:	Where are the records stored? Is there a centralised database of EHR? What security technology is being used?
Rights of the person/patient concerned:	How can the right of access be exercised? How can the data be corrected? Can the person enter information in his or her own EHR? What are the legal remedies available?
Consent:	Is the system based on an opt-in approach? Is the principle of granular consent applied (with the possibility of preventing access to certain data?)? If yes, in which situations?
Withdrawal:	Are patients able to withdraw the consent given to EHR schemes? If yes, what is the relevant procedure to withdraw such consent? What are the consequences?
Outsourcing processing of data:	Is outsourcing common? Under what circumstances? Where is the data outsourced to? What sort of safeguards are in place?

2. Cloud Computing, Data Mining and Profiling from both Medical Records (including EHR) and Data not specifically related to medical records.

2.1. Data Protection Issues:

Cloud computing has brought a new dimension to the way data is stored, accessed and processed. Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS), Network as a service (NaaS) are all used by services and organisations that deal with both medical data and non-medical data.

With the development of more advanced and efficient data-mining and data-querying Medical techniques (e.g NoSQL, MapReduce, Hadoop) in conjunction with increased processing power and data storage, mining data has never been more informative, easier, and cost-effective.

Healthcare is a natural sector in which to apply new technologies and methodologies, with particular impacts in epidemiology, public health, health services research, etc.

Data that can lead to the identification of a particular individual and his/her health situation is not limited to medical data *per se,* present on Electronic Health Records, but also to unsuspicious type of information.

There is a growing concern that these schemes may be implemented in manner which does not always respect the patients' confidentiality and basic rights, and in a broader context, the use of this of information may prejudice the individuals concerned.

The ability to track and monitor patients and resources enables a more efficient provision of care but may have an impact on the right to privacy of the individual concerned.

2.2. Questions: Is your legal framework providing for a regulation of Cloud Computing, Data Mining and Profiling? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Cloud computing:	How is cloud computing regulated in your country? Which security safeguards and standards are mandatory? Are there specific requirements in order to store medical data in the cloud? How is data shared and is the sharing regulated?
Government:	Do governmental programmes exist to allow for increased data-mining of medical records? If yes, what are the purposes of this data mining? Are private entities allowed to access the data? Under what circumstances? What sort of techniques and technologies are being used? To what end? Are data subjects informed of this type of data-mining?
Private sector:	Are private entities allowed to mine medical data which they process? Under what circumstances? Can the government have access to this data?
Profiling:	Are the government and the private sector allowed to employ profiling methods on medical data? If yes, under what circumstances? Is it allowed to cross and correlate non-medical data with medical data?

3. RFID and wireless communication technologies

3.1. Data Protection Issues:

It is common for medical devices, such as patients' tags, to possess RFID technologies in order to facilitate the transmission of the patients' data.

It can also be related to the data-mining operations previously mentioned as it is another category of information that can be used to discern meaningful patterns.

Transmission of data through radio-frequency is not limited to medical devices. Almost any smartphone uses some technology enabling to collect, and share, the user's data. For instance, via WI-FI it is possible to identify users' locations and therefore infer some of their behaviour, which in some cases can relate to health information.

3.2. Questions: Is your legal framework providing for a regulation of RFID technologies and the transfer of personal data through wireless technologies? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
RFID:	How is RFID used in hospital/clinics for (a) resource management, (b) patient care? What types of database systems (and security) are implemented in conjunction with RFID use? How are issues of access, sharing, consent etc. managed considering that RFID may be used without the patients' knowledge.
Wireless tracking technologies:	Are hospitals/clinics employing other wireless tracking technologies besides RFID? Which ones? Do they have to follow specific security requirements? Which ones?

4. Applications (Mobile)

4.1. Data Protection Issues: Information society is increasingly relying on the use of "apps" (application), most of them mobile. These apps are commonly designed to gather personal data, and in practice often process medical data. Technologies such as multi-touch touchscreen, accelerometers or gyroscopes, ambient light sensors, GPS and cameras, and devices featuring fingerprint and biometric sensors also involve the collection of medical data. A mobile phone application can monitor accurately physiological data, such as heartbeats, sleep patterns, fitness information.

4.2. Questions: Is your legal framework providing for a regulation of Apps and Mobile Apps? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Apps:	Is it allowed to use apps and mobile apps to deploy medical services and collect medical data? If yes, which type of individual/organisation can develop and employ these apps? Are there specific security requirements for these types of apps?

Institutions:	Do hospitals/clinics/labs employ apps to gather medical data? Is there a need for a medical treatment to permit the use of an app to process the medical data? Are there specific security requirements for the institutions collecting these data from the apps? Are medico-administrative data used by hospitals/clinics for management purposes?
Tracking technologies:	Do hospitals/clinics/labs employ non-medical apps and devices to track and collect data from their patients? What type of data is collected? For what purpose? Is the data identifiable? Is the data combined with medical data?
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical apps and tracking apps? If yes, what are the standards?
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical diagnostic? How would this be applied to fitness and daily-basis data?

5. Medical Devices and Wearable Devices

5.1. Data Protection Issues:

A medical device can be defined as: 'any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application. Such a device should be intended by the manufacturer for one of a number of defined purposes, one of which is, diagnosis, prevention, monitoring, treatment or alleviation of disease' (Directive 93/42/EEC Article 1:2)

Some eHealth and mHealth devices and apps do not fall in this definition of medical devices, as can also be the case of a software working in combination with a physical device, for instance a smartphone.

5.2. Questions: Is your legal framework providing for a regulation of Medical Devices? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
eHealth and mHealth:	Does the concept of Medical device in your country encompass services and apparels in the realm of eHealth and mHealth? What are the requirements? Should, for instance, the medical device be certified before it can be used?
Apps:	Does the concept of medical devices encompass apps? If yes, is there any regulation applicable to apps that perform medical services? Is there any regulation applicable on apps that track non-medical data that can lead to health information? If yes, what type of data?

Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical and/or wearable devices? If yes, what are the standards?
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical treatment? How would this be applied to fitness and daily-basis data?

6. Internet of Things

6.1. Data Protection Issues:

Internet of things relates to common, ordinary devices that are now, and increasingly, connected to the Internet, such as cars, fridges, ovens, microwaves, etc. All of these devices can provide data that can lead to reveal information concerning one's health. A fridge can easily inform on the type of food stored and thus the diet of an individual. One of the biggest challenges of the Internet of Things is to guarantee the right to privacy and data protection in a world where every device collects, processes, analyses and transmits the data, commonly via wireless technologies.

In the realm of medical data, the issue mainly arises when crossing seemly unrelated data that can lead to health information about an individual.

6.2. Questions: Is your legal framework providing for a regulation of the Internet of Things? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Security:	What are the security standards that need to be employed by these devices when collecting personal data?
Non-medical devices:	Are non-medical devices allowed to collect medical data, such as heart frequency? Are they allowed to cross medical data with non-medical data?
Privacy by Design:	Is there any requirement to implement privacy by design in the development of connected devices? If yes, what are the standards?

7. Electronic Doctor (online Doctor) and on-line appointments

7.1. Data Protection Issues:

The Doctor listens, talks and assesses the patient online, via a website, app, canal, sometimes including video-conference. Medical data is collected and processed, what are the security requirements and standards followed? Other websites provide for on-line appointments with doctors, which can also involve the processing of medical data.

7.2. Questions: Is your legal framework providing for a regulation of online Medical Treatment and is the on-line appointment system covered by such a framework? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Medical treatment:	Is it allowed to perform medical treatment via online services? If yes, how should the medical services be provided? Does it have to follow the same requirements of a regular physically-present medical treatment?
Medical data:	How should the data collected via a medical treatment performed online be processed? Are there specific requirements? Which ones?

Other comments and technologies
Should you wish to describe any technology, feature or trend that has not been covered by the questionnaire, please feel free to use the space provided below. Where relevant, also indicate recent legislation changes, guidelines and/or case law.

PRIVATE HEALTH CARE 5.

QUESTIONNAIRE

The questionnaire should ideally be completed by data protection authorities, health policy authorities, professional or patient associations as well as healthcare providers: you are invited to share it as widely as possible.

Please send your replies to dataprotection@coe.int no later than 15 December 2014.

1. Mobile Health (mHealth) and Electronic Health Records (EHR)

1.1. Data Protection Issues:

This is perhaps the biggest topic sitting at the intersection of technology and data protection. Mobile health (mHealth) and Electronic Health Records (EHR) are increasingly used in healthcare systems and provisions – it is a trend that needs to be examined.

Related to the EHR, these records are more accurate, cost-effective (in terms of storage) than paper-based notes. The concept of patient controlled/accessed EHR has been implemented in varying degrees in different countries.

Furthermore, some non-medical record can still contain health information about users and it should be considered if such records ought to be treated in a similar way to EHR.

Also, should 'medical data' as defined in Recommendation N° (97) 5 on the protection of medical data cover physical tracking data, such as pedometers or fitness data and data that can lead to medical information about an individual ?

1.2. Questions: if EHR exist in your country, is your legal framework providing for a regulation of such records? If mHealth exists in your country, is your legal framework providing for a specific regulation? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
EHR and Medical data:	What can be considered medical data in your country? Is it solely the data relating to a person's health (state, diagnosis, prognosis, medical treatment, etc.)? Is non-medical data that leads to medical information treated the same way as medical data (for instance in terms of confidentiality requirements)? Is the EHR solely constituted of data collected in a medical context or can the individual also himself or herself add information regarding his or her health?
	These are info considering the health of the people. Non-medical data are treated on same way as medical data due to confidence. EHR consists of data collected in medical context.
Sharing of data and Access:	Who is granted access to the EHR and how is the sharing of information (with other health care providers?) regulated? Where information is shared with pharmacists, is there a strict purpose limitation in place? How has the definition of the responsibility over the medical data been regulated?

	Sharing data can be only done by specific medical workers that are allowed to do that. Only certain info among the working sector are available.
Data quality:	Are the principles of legitimacy, fairness and minimization applied to medical data? How are records kept accurate? How long is the data kept for, is the specific storage period defined for the EHR?
	Principles of legitimacy and minimization are applied to medical data. Data should be kept minimum 5 years.
Data integrity:	Are any specific methods used to ensure the integrity of the data? How are patients identified in the EHR? In the context of research, are anonymisation methods used and what safeguards exist for re-identification?
	Patients are identified health card or ID cards.
Data security:	Where are the records stored? Is there a centralized database of EHR? What security technology is being used?
	Data is stored in health records (paper and in electronic form) and in medical and electronic diaries. Special codes for electronic data are used and only the authorized medical worker can access it. Paper data are locked in archives.
Rights of the person/patient concerned:	How can the right of access be exercised? How can the data be corrected? Can the person enter information in his or her own EHR? What are the legal remedies available?
	Access to patients' records has medical personnel. Patients could not enter data by themselves.
Consent:	Is the system based on an opt-in approach? Is the principle of granular consent applied (with the possibility of preventing access to certain data?)? If yes, in which situations?
	Principle of granular consent is applied.
Withdrawal:	Are patients able to withdraw the consent given to EHR schemes? If yes, what is the relevant procedure to withdraw such consent? What are the consequences?
	We think it is not allowed.
Outsourcing processing of data:	Is outsourcing common? Under what circumstances? Where is the data outsourced to? What sort of safeguards are in place?

2. Cloud Computing, Data Mining and Profiling from both Medical Records (including EHR) and Data not specifically related to medical records.

2.1. Data Protection Issues:

Cloud computing has brought a new dimension to the way data is stored, accessed and processed. Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS), Network as a service (NaaS) are all used by services and organisations that deal with both medical data and non-medical data.

With the development of more advanced and efficient data-mining and data-querying Medical techniques (e.g NoSQL, MapReduce, Hadoop) in conjunction with increased processing power and data storage, mining data has never been more informative, easier, and cost-effective.

Healthcare is a natural sector in which to apply new technologies and methodologies, with particular impacts in epidemiology, public health, health services research, etc.

Data that can lead to the identification of a particular individual and his/her health situation is not limited to medical data *per se,* present on Electronic Health Records, but also to unsuspicious type of information.

There is a growing concern that these schemes may be implemented in manner which does not always respect the patients' confidentiality and basic rights, and in a broader context, the use of this of information may prejudice the individuals concerned.

The ability to track and monitor patients and resources enables a more efficient provision of care but may have an impact on the right to privacy of the individual concerned.

2.2. Questions: Is your legal framework providing for a regulation of Cloud Computing, Data Mining and Profiling? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Cloud computing:	How is cloud computing regulated in your country? Which security safeguards and standards are mandatory? Are there specific requirements in order to store medical data in the cloud? How data is shared and is the sharing regulated?
	There are specific requests where data should be locked with codes and authorized people can use it when necessary.
Government:	Do governmental programs exist to allow for increased data-mining of medical records? If yes, what are the purposes of this data mining? Are private entities allowed to access the data? Under what circumstances? What sort of techniques and technologies are being used? To what end? Are data subjects informed of this type of data-mining?
Private sector:	Are private entities allowed to mine medical data which they process? Under what circumstances? Can the government have access to this data?
Profiling:	Are the government and the private sector allowed to employ profiling methods on medical data? If yes, under what circumstances? Is it allowed to cross and correlate non-medical data with medical data?

3. RFID and wireless communication technologies

3.1. Data Protection Issues:

It is common for medical devices, such as patients' tags, to possess RFID technologies in order to facilitate the transmission of the patients' data.

It can also be related to the data-mining operations previously mentioned as it is another category of information that can be used to discern meaningful patterns.

Transmission of data through radio-frequency is not limited to medical devices. Almost any smartphone uses some technology enabling to collect, and share, the user's data. For instance, via WI-FI it is possible to identify users' locations and therefore infer some of their behaviour, which in some cases can relate to health information.

3.2. Questions: Is your legal framework providing for a regulation of RFID technologies and the transfer of personal data through wireless technologies? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
RFID:	How is RFID used in hospital/clinics for (a) resource management, (b) patient care? What types of database systems (and security) are implemented in conjunction with RFID use? How are issues of access, sharing, consent etc. managed considering that RFID may be used without the patients' knowledge.
Wireless tracking technologies:	Are hospitals/clinics employing other wireless tracking technologies besides RFID? Which ones? Do they have to follow specific security requirements? Which ones?

4. Applications (Mobile)

4.1. Data Protection Issues:

Information society is increasingly relying on the use of "apps" (application), most of them mobile. These apps are commonly designed to gather personal data, and in practice often process medical data.
Technologies such as multi-touch touchscreen, accelerometers or gyroscopes, ambient light sensors, GPS and cameras, and devices featuring fingerprint and biometric sensors also involve the collection of medical data.

A mobile phone application can monitor accurately physiological data, such as heartbeats, sleep patterns, fitness information.

4.2. Questions: Is your legal framework providing for a regulation of Apps and Mobile Apps? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).

Apps:	Is it allowed to use apps and mobile apps to deploy medical services and collect medical data? If yes, which type of individual/organisation can develop and employ these apps? Are there specific security requirements for these types of apps?
Institutions:	Do hospitals/clinics/labs employ apps to gather medical data? Is there a need for a medical treatment to permit the use of an app to process the medical data? Are there specific security requirements for the institutions collecting these data from the apps? Are medico-administrative data used by hospitals/clinics for management purposes?
Tracking technologies:	Do hospitals/clinics/labs employ non-medical apps and devices to track and collect data from their patients? What type of data is collected? For what purpose? Is the data identifiable? Is the data combined with medical data?
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical apps and tracking apps? If yes, what are the standards?
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical diagnostic? How would this be applied to fitness and daily-basis data?

5. Medical Devices and Wearable Devices

5.1. Data Protection Issues:

A medical device can be defined as: 'any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application. Such a device should be intended by the manufacturer for one of a number of defined purposes, one of which is, diagnosis, prevention, monitoring, treatment or alleviation of disease' (Directive 93/42/EEC Article 1:2)

Some eHealth and mHealth devices and apps do not fall in this definition of medical devices, as can also be the case of a software working in combination with a physical device, for instance a smartphone.

5.2. Questions: Is your legal framework providing for a regulation of Medical Devices? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	No.
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
eHealth and mHealth:	Does the concept of Medical device in your country encompass services and apparels in the realm of eHealth and mHealth? What are the requirements? Should, for instance, the medical device be certified before it can be used?
	NO info.
Apps:	Does the concept of medical devices encompass apps? If yes, is there any regulation applicable to apps that perform medical services? Is there any regulation applicable on apps that track non-medical data that can lead to health information? If yes, what type of data?
	NO info.
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical and/or wearable devices? If yes, what are the standards?
	Log in and firewall.
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical treatment? How would this be applied to fitness and daily-basis data?
	NO info.

6. Internet of Things

6.1. Data Protection Issues:

Internet of things relates to common, ordinary devices that are now, and increasingly, connected to the Internet, such as cars, fridges, ovens, microwaves, etc. All of these devices can provide data that can lead to reveal information concerning one's health. A fridge can easily inform on the type of food stored and thus the diet of an individual. One of the biggest challenges of the Internet of Things is to guarantee the right to privacy and data protection in a world where every device collects, processes, analyses and transmits the data, commonly via wireless technologies.

In the realm of medical data, the issue mainly arises when crossing seemly unrelated data that can lead to health information about an individual.

6.2. Questions: Is your legal framework providing for a regulation of the Internet of Things? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	NO info.
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Security:	What are the security standards that need to be employed by these devices when collecting personal data?
	NO info.

Non-medical devices:	Are non-medical devices allowed to collect medical data, such as heart frequency? Are they allowed to cross medical data with non-medical data?
	NO info.
Privacy by Design:	Is there any requirement to implement privacy by design in the development of connected devices? If yes, what are the standards?
	NO info.

7. Electronic Doctor (online Doctor) and on-line appointments

7.1. Data Protection Issues:

The Doctor listens, talks and assesses the patient online, via a website, app, canal, sometimes including video-conference. Medical data is collected and processed, what are the security requirements and standards followed? Other websites provide for on-line appointments with doctors, which can also involve the processing of medical data.

7.2. Questions: Is your legal framework providing for a regulation of online Medical Treatment and is the on-line appointment system covered by such a framework? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	There are no online medical examinations.
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Medical treatment:	Is it allowed to perform medical treatment via online services? If yes, how should the medical services be provided? Does it have to follow the same requirements of a regular physically-present medical treatment?
	No
Medical data:	How should the data collected via a medical treatment performed online be processed? Are there specific requirements? Which ones?
	No info.

Other comments and technologies
Should you wish to describe any technology, feature or trend that has not been covered by the questionnaire, please feel free to use the space provided below. Where relevant, also indicate recent legislation changes, guidelines and/or case law.

PRIVATE HEALTH CARE 6.

QUESTIONNAIRE

The questionnaire should ideally be completed by data protection authorities, health policy authorities, professional or patient associations as well as healthcare providers: you are invited to share it as widely as possible.

Please send your replies to dataprotection@coe.int no later than 15 December 2014.

1. Mobile Health (mHealth) and Electronic Health Records (EHR)

1.1. Data Protection Issues:

This is perhaps the biggest topic sitting at the intersection of technology and data protection. Mobile health (mHealth) and Electronic Health Records (EHR) are increasingly used in healthcare systems and provisions – it is a trend that needs to be examined.

Related to the EHR, these records are more accurate, cost-effective (in terms of storage) than paper-based notes. The concept of patient controlled/accessed EHR has been implemented in varying degrees in different countries.

Furthermore, some non-medical record can still contain health information about users and it should be considered if such records ought to be treated in a similar way to EHR.

Also, should 'medical data' as defined in Recommendation N° (97) 5 on the protection of medical data cover physical tracking data, such as pedometers or fitness data and data that can lead to medical information about an individual ?

1.2. Questions: if EHR exist in your country, is your legal framework providing for a regulation of such records? If mHealth exists in your country, is your legal framework providing for a specific regulation? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
EHR and Medical data:	What can be considered medical data in your country? Is it solely the data relating to a person's health (state, diagnosis, prognosis, medical treatment, etc.)? Is non-medical data that leads to medical information treated the same way as medical data (for instance in terms of confidentiality requirements)? Is the EHR solely constituted of data collected in a medical context or can the individual also himself or herself add information regarding his or her health?
	Medical data is data relating to the health of the individual and includes data concerning the history, diagnosis, prognosis and treatment, as well as data that have a clear and close relationship with health Art. 2, paragraph 1, item 9 of the records in the field of health Non-medical data concerning the health status of an individual is treated in the same way as medical data (in terms of baranjata confidentiality. Art. 25 of the law to protect the rights of patients.

	The right to confidentiality (secrecy) have personal and medical data, which must be kept secret after the death of the patient, in accordance with the regulations for the protection of personal data The medical record contains data from patients who have the right to provide information about his health. (History). But they kept on paper and not electronically recorded. Art. 12 paragraphs 2 and 3 of the records in the area of health: Enrollment data means for keeping records on the basis of the results of the review and documentation of the health institution or the public and other documents. If the data can not be saved in funds for running the records as specified in paragraph (2) of this Article shall be recorded on the statement of the person who is taking the data entered in the records.(anamneza)
Sharing of data and Access:	Who is granted access to the EHR and how is the sharing of information (with other health care providers?) regulated? Where information is shared with pharmacists, is there a strict purpose limitation in place? How has the definition of the responsibility over the medical data been regulated?
	EMR is available only to persons by the director of the institution received special authorization and signed a declaration of confidentiality, in accordance with the Law on Protection of Personal podatci. Sharing data is performed only with institutions that are legally determined to use the data, which are central to public health, the Fund and the Ministry of Health. Personal data will be transmitted via electronic communications network from the hospital to the Health Insurance Fund, Center for Public Health and the Ministry of Health, which contain a unique identification number and other protected data is encrypted and protected with appropriate measures to ensure that the data not readable in transit. Data with pharmacists in our institution are not shared yet, it goes through family doctors. Responsibility for medical data is defined as professional secrecy. In it there are clauses in employment contracts.
Data quality:	Are the principles of legitimacy, fairness and minimization applied to medical data? How are records kept accurate? How long is the data kept for, is the specific storage period defined for the EHR?
	Yes, there is. Personal details only if prescribed by law. Some data such as medical data relating to biomedical assisted fertilization are no legal limits for storage and the other as the assessment of the user are stored on a period on Provisions for filing and regulations for classified information.
Data integrity:	Are any specific methods used to ensure the integrity of the data? How are patients identified in the EHR? In the context of research, are anonymisation methods used and what safeguards exist for re-identification?
	There are safeguards in accordance with the Law on the protection of personal data. Identification of patient EMR is done based on the registration number, sex, nationality and other special categories of data pursuant to the records relating to health are collected in form of medical records.
Data security:	Where are the records stored? Is there a centralized database of EHR? What security technology is being used?
	Stored in the software and security copies.

Rights of the person/patient concerned:	How can the right of access be exercised? How can the data be corrected? Can the person enter information in his or her own EHR? What are the legal remedies available?
	Only on the basis of a written request of the patient. The other party can not give information of EMR unless a patient Statement on persons who can give information about the disease. The patient should be given a written or oral statement to those who can give information about his admission to hospital health facility, or statement of a person for further communication, as well as his health, or for people who do not dare to give such information community in which he lives. - Excerpt from the Law on Protection of Patients' Rights. The patient can not enter information in its EMR, it can be made only by authorized officer.
Consent:	Is the system based on an opt-in approach? Is the principle of granular consent applied (with the possibility of preventing access to certain data?)? If yes, in which situations?
	The hospital, check for any unauthorized access to an authorized person who has access to records of personal data with the following data: - Name of authorized person - Workstation - Where accessing information system, - Date and time of entry, - To the personal data that is accessed, - The type of access operations undertaken in processing data, - Record of authorization for each accession - Record of any unauthorized access and record of automated rejection of the information system
Withdrawal:	Are patients able to withdraw the consent given to EHR schemes? If yes, what is the relevant procedure to withdraw such consent? What are the consequences?
	It is not allowed. Data is used for statistical purposes also.
Outsourcing processing of data:	Is outsourcing common? Under what circumstances? Where is the data outsourced to? What sort of safeguards are in place?
	It is not allowed.

2. Cloud Computing, Data Mining and Profiling from both Medical Records (including EHR) and Data not specifically related to medical records.

2.1. Data Protection Issues:

Cloud computing has brought a new dimension to the way data is stored, accessed and processed. Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS), Network as a service (NaaS) are all used by services and organisations that deal with both medical data and non-medical data.

With the development of more advanced and efficient data-mining and data-querying Medical techniques (e.g NoSQL, MapReduce, Hadoop) in conjunction with increased processing power and data storage, mining data has never been more informative, easier, and cost-effective.

Healthcare is a natural sector in which to apply new technologies and methodologies, with particular impacts in epidemiology, public health, health services research, etc.

Data that can lead to the identification of a particular individual and his/her health situation is not limited to medical data *per se,* present on Electronic Health Records, but also to unsuspicious type of information.

There is a growing concern that these schemes may be implemented in manner which does not always respect the patients' confidentiality and basic rights, and in a broader context, the use of this of information may prejudice the individuals concerned.

The ability to track and monitor patients and resources enables a more efficient provision of care but may have an impact on the right to privacy of the individual concerned.

2.2. Questions: Is your legal framework providing for a regulation of Cloud Computing, Data Mining and Profiling? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Cloud computing:	How is cloud computing regulated in your country? Which security safeguards and standards are mandatory? Are there specific requirements in order to store medical data in the cloud? How data is shared and is the sharing regulated?
	The data is not stored in the cloud, the data stored in local server stationed at the hospital.
Government:	Do governmental programs exist to allow for increased data-mining of medical records? If yes, what are the purposes of this data mining? Are private entities allowed to access the data? Under what circumstances? What sort of techniques and technologies are being used? To what end? Are data subjects informed of this type of data-mining?
	We are not familiar with government programs that will respond to rising mining medical data
Private sector:	Are private entities allowed to mine medical data which they process? Under what circumstances? Can the government have access to this data?
	Medical data are subject to mining of any private entity.
Profiling:	Are the government and the private sector allowed to employ profiling methods on medical data? If yes, under what circumstances? Is it allowed to cross and correlate non-medical data with medical data?
	We are not familiar with the permit if the government and the private sector are allowed to use the methods of profiling of medical data.

3. RFID and wireless communication technologies

3.1. Data Protection Issues:

It is common for medical devices, such as patients' tags, to possess RFID technologies in order to facilitate the transmission of the patients' data.

It can also be related to the data-mining operations previously mentioned as it is another category of information that can be used to discern meaningful patterns.

Transmission of data through radio-frequency is not limited to medical devices. Almost any smartphone uses some technology enabling to collect, and share, the user's data. For instance, via

WI-FI it is possible to identify users' locations and therefore infer some of their behaviour, which in some cases can relate to health information.

3.2. Questions: Is your legal framework providing for a regulation of RFID technologies and the transfer of personal data through wireless technologies? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	Access to data is regulated by local LAN network, server and router are protected Firewall that limit the access them
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
RFID:	How is RFID used in hospital/clinics for (a) resource management, (b) patient care? What types of database systems (and security) are implemented in conjunction with RFID use? How are issues of access, sharing, consent etc. managed considering that RFID may be used without the patients' knowledge.
	RFID is not used in the resource management system of the hospital
Wireless tracking technologies:	Are hospitals/clinics employing other wireless tracking technologies besides RFID? Which ones? Do they have to follow specific security requirements? Which ones?

4. Applications (Mobile)

4.1. Data Protection Issues:

Information society is increasingly relying on the use of "apps" (application), most of them mobile. These apps are commonly designed to gather personal data, and in practice often process medical data.
Technologies such as multi-touch touchscreen, accelerometers or gyroscopes, ambient light sensors, GPS and cameras, and devices featuring fingerprint and biometric sensors also involve the collection of medical data.

A mobile phone application can monitor accurately physiological data, such as heartbeats, sleep patterns, fitness information.

4.2. Questions: Is your legal framework providing for a regulation of Apps and Mobile Apps? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	The hospital did not use mobile applications and management of patients' data
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Apps:	Is it allowed to use apps and mobile apps to deploy medical services and collect medical data? If yes, which type of individual/organisation can develop and employ these apps? Are there specific security requirements for these types of apps?
	No

Institutions:	Do hospitals/clinics/labs employ apps to gather medical data? Is there a need for a medical treatment to permit the use of an app to process the medical data? Are there specific security requirements for the institutions collecting these data from the apps? Are medico-administrative data used by hospitals/clinics for management purposes?
Tracking technologies:	Do hospitals/clinics/labs employ non-medical apps and devices to track and collect data from their patients? What type of data is collected? For what purpose? Is the data identifiable? Is the data combined with medical data?
	The hospital don't use such a technology.
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical apps and tracking apps? If yes, what are the standards?
	There are requirements for the implementation of privacy by design in the process of developing medical applications according to the standards defined in Article 41 and line 4 of the Law on Protection of Personal Data
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical diagnostic? How would this be applied to fitness and daily-basis data?
	There is no opt-in possibility.

5. Medical Devices and Wearable Devices

5.1. Data Protection Issues:

A medical device can be defined as: 'any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application. Such a device should be intended by the manufacturer for one of a number of defined purposes, one of which is, diagnosis, prevention, monitoring, treatment or alleviation of disease' (Directive 93/42/EEC Article 1:2)

Some eHealth and mHealth devices and apps do not fall in this definition of medical devices, as can also be the case of a software working in combination with a physical device, for instance a smartphone.

5.2. Questions: Is your legal framework providing for a regulation of Medical Devices? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
eHealth and mHealth:	Does the concept of Medical device in your country encompass services and apparels in the realm of eHealth and mHealth? What are the requirements? Should, for instance, the medical device be certified before it can be used?

Apps:	Does the concept of medical devices encompass apps? If yes, is there any regulation applicable to apps that perform medical services? Is there any regulation applicable on apps that track non-medical data that can lead to health information? If yes, what type of data?
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical and/or wearable devices? If yes, what are the standards?
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical treatment? How would this be applied to fitness and daily-basis data?

6. Internet of Things

6.1. Data Protection Issues:

Internet of things relates to common, ordinary devices that are now, and increasingly, connected to the Internet, such as cars, fridges, ovens, microwaves, etc. All of these devices can provide data that can lead to reveal information concerning one's health. A fridge can easily inform on the type of food stored and thus the diet of an individual. One of the biggest challenges of the Internet of Things is to guarantee the right to privacy and data protection in a world where every device collects, processes, analyses and transmits the data, commonly via wireless technologies.

In the realm of medical data, the issue mainly arises when crossing seemly unrelated data that can lead to health information about an individual.

6.2. Questions: Is your legal framework providing for a regulation of the Internet of Things? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Security:	What are the security standards that need to be employed by these devices when collecting personal data?
Non-medical devices:	Are non-medical devices allowed to collect medical data, such as heart frequency? Are they allowed to cross medical data with non-medical data?
Privacy by Design:	Is there any requirement to implement privacy by design in the development of connected devices? If yes, what are the standards?

7. Electronic Doctor (online Doctor) and on-line appointments

7.1. Data Protection Issues:
The Doctor listens, talks and assesses the patient online, via a website, app, canal, sometimes including video-conference. Medical data is collected and processed, what are the security requirements and standards followed? Other websites provide for on-line appointments with doctors, which can also involve the processing of medical data.

7.2. Questions: Is your legal framework providing for a regulation of online Medical Treatment and is the on-line appointment system covered by such a framework? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	There are no online medical examinations.
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Medical treatment:	Is it allowed to perform medical treatment via online services? If yes, how should the medical services be provided? Does it have to follow the same requirements of a regular physically-present medical treatment?
	No
Medical data:	How should the data collected via a medical treatment performed online be processed? Are there specific requirements? Which ones?
	No info.

Other comments and technologies
Should you wish to describe any technology, feature or trend that has not been covered by the questionnaire, please feel free to use the space provided below. Where relevant, also indicate recent legislation changes, guidelines and/or case law.

PRIVATE HEALTH CARE 7.

QUESTIONNAIRE

The questionnaire should ideally be completed by data protection authorities, health policy authorities, professional or patient associations as well as healthcare providers: you are invited to share it as widely as possible.

Please send your replies to dataprotection@coe.int no later than 15 December 2014.

1. Mobile Health (mHealth) and Electronic Health Records (EHR)

1.1. Data Protection Issues:
This is perhaps the biggest topic sitting at the intersection of technology and data protection. Mobile health (mHealth) and Electronic Health Records (EHR) are increasingly used in healthcare systems and provisions – it is a trend that needs to be examined. Related to the EHR, these records are more accurate, cost-effective (in terms of storage) than paper-based notes. The concept of patient controlled/accessed EHR has been implemented in varying degrees in different countries. Furthermore, some non-medical record can still contain health information about users and it should be considered if such records ought to be treated in a similar way to EHR. Also, should 'medical data' as defined in Recommendation N° (97) 5 on the protection of medical data cover physical tracking data, such as pedometers or fitness data and data that can lead to medical information about an individual ?

1.2. Questions: if EHR exist in your country, is your legal framework providing for a regulation of such records? If mHealth exists in your country, is your legal framework providing for a specific regulation? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	In RM there is a legislation for medical records with responding legal framework. It is regulated by the Health insurance fund of RM as well as data protection regulated by DPDP.
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
EHR and Medical data:	What can be considered medical data in your country? Is it solely the data relating to a person's health (state, diagnosis, prognosis, medical treatment, etc.)? Is non-medical data that leads to medical information treated the same way as medical data (for instance in terms of confidentiality requirements)? Is the EHR solely constituted of data collected in a medical context or can the individual also himself or herself add information regarding his or her health?
	All data that is in patients' records are in accordance with the performed intervention. On this data is added the ID data and health data .All data is confidentially treated.
Sharing of data and Access:	Who is granted access to the EHR and how is the sharing of information (with other health care providers?) regulated? Where information is shared with pharmacists, is there a strict purpose limitation in place? How has the definition of

	the responsibility over the medical data been regulated?
	The access is allowed to the doctors and other medical personnel that have secured access. Information is not shared. Data that is shared with pharmacists is given by the patient according the medical services. Their responsibility is regulated with contract and legal provisions from Health insurance fund of RM as well as legal provisions of DPDP.
Data quality:	Are the principles of legitimacy, fairness and minimization applied to medical data? How are records kept accurate? How long is the data kept for, is the specific storage period defined for the EHR?
	All legitimacy principles are respected and implemented. Data is updated in written form and electronic form. There is no due date for data storage, having in mind that every patient should have medical history in one institution. Excluding the records for death, those data is erased.
Data integrity:	Are any specific methods used to ensure the integrity of the data? How are patients identified in the EHR? In the context of research, are anonymisation methods used and what safeguards exist for re-identification?
	All methods are previously determined. Patients are determined with ID number and unique number of insured person.
Data security:	Where are the records stored? Is there a centralized database of EHR? What security technology is being used?
	There is centralized data base in every health institution as well as HER on web portal of Health insurance fund of RM. There is appropriate protection .
Rights of the person/patient concerned:	How can the right of access be exercised? How can the data be corrected? Can the person enter information in his or her own EHR? What are the legal remedies available?
	Only medical personnel have access to data. The individual can check his data and ask for changes if necessary.
Consent:	Is the system based on an opt-in approach? Is the principle of granular consent applied (with the possibility of preventing access to certain data?)? If yes, in which situations?
	The principle of granular consent is applied because of the sensitivity of data and the need of data from the personnel. The health insurance fund also applies granular consent because only authorized employees could access the data base.
Withdrawal:	Are patients able to withdraw the consent given to EHR schemes? If yes, what is the relevant procedure to withdraw such consent? What are the consequences?
	The patient has the right to withdraw the consent for HER without consequences, Only info for performed interventions should be kept within the medical institution.
Outsourcing processing of data:	Is outsourcing common? Under what circumstances? Where is the data outsourced to? What sort of safeguards are in place?

2. Cloud Computing, Data Mining and Profiling from both Medical Records (including EHR) and Data not specifically related to medical records.

2.1. Data Protection Issues:

Cloud computing has brought a new dimension to the way data is stored, accessed and processed. Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS), Network as a service (NaaS) are all used by services and organisations that deal with both medical data and non-medical data.

With the development of more advanced and efficient data-mining and data-querying Medical techniques (e.g NoSQL, MapReduce, Hadoop) in conjunction with increased processing power and data storage, mining data has never been more informative, easier, and cost-effective.

Healthcare is a natural sector in which to apply new technologies and methodologies, with particular impacts in epidemiology, public health, health services research, etc.

Data that can lead to the identification of a particular individual and his/her health situation is not limited to medical data *per se,* present on Electronic Health Records, but also to unsuspicious type of information.

There is a growing concern that these schemes may be implemented in manner which does not always respect the patients' confidentiality and basic rights, and in a broader context, the use of this of information may prejudice the individuals concerned.

The ability to track and monitor patients and resources enables a more efficient provision of care but may have an impact on the right to privacy of the individual concerned.

2.2. Questions: Is your legal framework providing for a regulation of Cloud Computing, Data Mining and Profiling? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Cloud computing:	How is cloud computing regulated in your country? Which security safeguards and standards are mandatory? Are there specific requirements in order to store medical data in the cloud? How is data shared and is the sharing regulated?
Government:	Do governmental programs exist to allow for increased data-mining of medical records? If yes, what are the purposes of this data mining? Are private entities allowed to access the data? Under what circumstances? What sort of techniques and technologies are being used? To what end? Are data subjects informed of this type of data-mining?
	We don't have enough info upon this question. But it will be great if there is a single data base.
Private sector:	Are private entities allowed to mine medical data which they process? Under what circumstances? Can the government have access to this data?
	Yes in case when medical history is needed. Yes, the government can access this info.
Profiling:	Are the government and the private sector allowed to employ profiling methods on medical data? If yes, under what circumstances? Is it allowed to cross and correlate non-medical data with medical data?

	It is not needed to cross and correlate non-medical and medical data in one medical institution.

3. RFID and wireless communication technologies

3.1. Data Protection Issues:

It is common for medical devices, such as patients' tags, to possess RFID technologies in order to facilitate the transmission of the patients' data.

It can also be related to the data-mining operations previously mentioned as it is another category of information that can be used to discern meaningful patterns.

Transmission of data through radio-frequency is not limited to medical devices. Almost any smartphone uses some technology enabling to collect, and share, the user's data. For instance, via WI-FI it is possible to identify users' locations and therefore infer some of their behaviour, which in some cases can relate to health information.

3.2. Questions: Is your legal framework providing for a regulation of RFID technologies and the transfer of personal data through wireless technologies? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	Wireless technologies could only be used in case of legal liability for data records. The responsible person perform that responsibility.
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
RFID:	How is RFID used in hospital/clinics for (a) resource management, (b) patient care? What types of database systems (and security) are implemented in conjunction with RFID use? How are issues of access, sharing, consent etc. managed considering that RFID may be used without the patients' knowledge.
	We don't have such info.
Wireless tracking technologies:	Are hospitals/clinics employing other wireless tracking technologies besides RFID? Which ones? Do they have to follow specific security requirements? Which ones?
	NO info.

4. Applications (Mobile)

4.1. Data Protection Issues:

Information society is increasingly relying on the use of "apps" (application), most of them mobile. These apps are commonly designed to gather personal data, and in practice often process medical data.
Technologies such as multi-touch touchscreen, accelerometers or gyroscopes, ambient light sensors, GPS and cameras, and devices featuring fingerprint and biometric sensors also involve the collection of medical data.

A mobile phone application can monitor accurately physiological data, such as heartbeats, sleep patterns, fitness information.

4.2. Questions: Is your legal framework providing for a regulation of Apps and Mobile Apps? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	All apps are regulated by selective access with appropriate consent and agreement.
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Apps:	Is it allowed to use apps and mobile apps to deploy medical services and collect medical data? If yes, which type of individual/organisation can develop and employ these apps? Are there specific security requirements for these types of apps?
	Every medical institution.
Institutions:	Do hospitals/clinics/labs employ apps to gather medical data? Is there a need for a medical treatment to permit the use of an app to process the medical data? Are there specific security requirements for the institutions collecting these data from the apps? Are medico-administrative data used by hospitals/clinics for management purposes?
	Yes, apps are used because of the performance of medical interventions. There are safety measures.
Tracking technologies:	Do hospitals/clinics/labs employ non-medical apps and devices to track and collect data from their patients? What type of data is collected? For what purpose? Is the data identifiable? Is the data combined with medical data?
	All non-medical data records are only for the purpose for identification.
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical apps and tracking apps? If yes, what are the standards?
	NO
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical diagnostic? How would this be applied to fitness and daily-basis data?
	Those are only data for identification and medical data , without any impact on the rest of the data.

5. Medical Devices and Wearable Devices

5.1. Data Protection Issues:

A medical device can be defined as: 'any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application. Such a device should be intended by the manufacturer for one of a number of defined purposes, one of which is, diagnosis, prevention, monitoring, treatment or alleviation of disease' (Directive 93/42/EEC Article 1:2)

Some eHealth and mHealth devices and apps do not fall in this definition of medical devices, as can also be the case of a software working in combination with a physical device, for instance a smartphone.

5.2. Questions: Is your legal framework providing for a regulation of Medical Devices? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	Every device is regulated and checked by the Ministry of health.
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
eHealth and mHealth:	Does the concept of Medical device in your country encompass services and apparels in the realm of eHealth and mHealth? What are the requirements? Should, for instance, the medical device be certified before it can be used?
	NO
Apps:	Does the concept of medical devices encompass apps? If yes, is there any regulation applicable to apps that perform medical services? Is there any regulation applicable on apps that track non-medical data that can lead to health information? If yes, what type of data?
	NO
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical and/or wearable devices? If yes, what are the standards?
	NO
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical treatment? How would this be applied to fitness and daily-basis data?

6. Internet of Things

6.1. Data Protection Issues:

Internet of things relates to common, ordinary devices that are now, and increasingly, connected to the Internet, such as cars, fridges, ovens, microwaves, etc. All of these devices can provide data that can lead to reveal information concerning one's health. A fridge can easily inform on the type of food stored and thus the diet of an individual. One of the biggest challenges of the Internet of Things is to guarantee the right to privacy and data protection in a world where every device collects, processes, analyses and transmits the data, commonly via wireless technologies.

In the realm of medical data, the issue mainly arises when crossing seemly unrelated data that can lead to health information about an individual.

6.2. Questions: Is your legal framework providing for a regulation of the Internet of Things? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	YES
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Security:	What are the security standards that need to be employed by these devices when collecting personal data?
	Agreements with producers and maintaining companies, based on legal liabilities according to the Law.
Non-medical devices:	Are non-medical devices allowed to collect medical data, such as heart frequency? Are they allowed to cross medical data with non-medical data?
	NO
Privacy by Design:	Is there any requirement to implement privacy by design in the development of connected devices? If yes, what are the standards?
	NO

7. Electronic Doctor (online Doctor) and on-line appointments

7.1. Data Protection Issues:

The Doctor listens, talks and assesses the patient online, via a website, app, canal, sometimes including video-conference. Medical data is collected and processed, what are the security requirements and standards followed? Other websites provide for on-line appointments with doctors, which can also involve the processing of medical data.

7.2. Questions: Is your legal framework providing for a regulation of online Medical Treatment and is the on-line appointment system covered by such a framework? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	
Case-law:	
Other:	NO, because it is about dental services which is impossible to be done online.

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Medical treatment:	Is it allowed to perform medical treatment via online services? If yes, how should the medical services be provided? Does it have to follow the same requirements of a regular physically-present medical treatment?
	No info.
Medical data:	How should the data collected via a medical treatment performed online be processed? Are there specific requirements? Which ones?
	No info.

Other comments and technologies
Should you wish to describe any technology, feature or trend that has not been covered by the questionnaire, please feel free to use the space provided below. Where relevant, also indicate recent legislation changes, guidelines and/or case law.
I think everything is covered.

PRIVATE HEALTH CARE 8.

QUESTIONNAIRE

The questionnaire should ideally be completed by data protection authorities, health policy authorities, professional or patient associations as well as healthcare providers: you are invited to share it as widely as possible.

Please send your replies to dataprotection@coe.int no later than 15 December 2014.

1. Mobile Health (mHealth) and Electronic Health Records (EHR)

1.1. Data Protection Issues:

This is perhaps the biggest topic sitting at the intersection of technology and data protection. Mobile health (mHealth) and Electronic Health Records (EHR) are increasingly used in healthcare systems and provisions – it is a trend that needs to be examined.

Related to the EHR, these records are more accurate, cost-effective (in terms of storage) than paper-based notes. The concept of patient controlled/accessed EHR has been implemented in varying degrees in different countries.

Furthermore, some non-medical record can still contain health information about users and it should be considered if such records ought to be treated in a similar way to EHR.

Also, should 'medical data' as defined in Recommendation N° (97) 5 on the protection of medical data cover physical tracking data, such as pedometers or fitness data and data that can lead to medical information about an individual ?

1.2. Questions: if EHR exist in your country, is your legal framework providing for a regulation of such records? If mHealth exists in your country, is your legal framework providing for a specific regulation? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	We don't have any info if there is specific legal regulative for HER, because we use already prepared medical reports from the Ministry of health.
Case-law:	We don't know.
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
EHR and Medical data:	What can be considered medical data in your country? Is it solely the data relating to a person's health (state, diagnosis, prognosis, medical treatment, etc.)? Is non-medical data that leads to medical information treated the same way as medical data (for instance in terms of confidentiality requirements)? Is the EHR solely constituted of data collected in a medical context or can the individual also himself or herself add information regarding his or her health?
	We think that medical and non-medical data for patients are treated in same way due to privacy. For now, only medical personnel (doctros) can add health data for the patient.
Sharing of data and Access:	Who is granted access to the EHR and how is the sharing of information (with other health care providers?) regulated? Where information is shared with pharmacists, is there a strict purpose limitation in place? How has the definition of

	the responsibility over the medical data been regulated?
	Only to medical personnel (doctors and assistants). We don't have info for pharmacists. .
Data quality:	Are the principles of legitimacy, fairness and minimization applied to medical data? How are records kept accurate? How long is the data kept for, is the specific storage period defined for the EHR?
	Only medical personnel could have access to data updates. For period of electronic data storage we don't have info, the paper documents are kept between 5 and 10 years.
Data integrity:	Are any specific methods used to ensure the integrity of the data? How are patients identified in the EHR? In the context of research, are anonymisation methods used and what safeguards exist for re-identification?
	We consider it no logical that the system Moj termin can be accessed from all devices, including smart phones, which is not OK. You can log in from different computers, including internet café where can be downloaded info for the patients. Patients are identified by e-cards or health card.
Data security:	Where are the records stored? Is there a centralized database of EHR? What security technology is being used?
	The system of the Ministry of health is web-based and data is stored on servers. We don't have info for security technologies. .
Rights of the person/patient concerned:	How can the right of access be exercised? How can the data be corrected? Can the person enter information in his or her own EHR? What are the legal remedies available?
	Access to patients' records has medical personnel. Patients could not enter data by themselves. We don't have info for legal assets.
Consent:	Is the system based on an opt-in approach? Is the principle of granular consent applied (with the possibility of preventing access to certain data?)? If yes, in which situations?
	No info.
Withdrawal:	Are patients able to withdraw the consent given to EHR schemes? If yes, what is the relevant procedure to withdraw such consent? What are the consequences?
	No info.
Outsourcing processing of data:	Is outsourcing common? Under what circumstances? Where is the data outsourced to? What sort of safeguards are in place?
	No info.

2. Cloud Computing, Data Mining and Profiling from both Medical Records (including EHR) and Data not specifically related to medical records.

2.1. Data Protection Issues:

Cloud computing has brought a new dimension to the way data is stored, accessed and processed. Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS),

Network as a service (NaaS) are all used by services and organisations that deal with both medical data and non-medical data.

With the development of more advanced and efficient data-mining and data-querying Medical techniques (e.g NoSQL, MapReduce, Hadoop) in conjunction with increased processing power and data storage, mining data has never been more informative, easier, and cost-effective.

Healthcare is a natural sector in which to apply new technologies and methodologies, with particular impacts in epidemiology, public health, health services research, etc.

Data that can lead to the identification of a particular individual and his/her health situation is not limited to medical data *per se,* present on Electronic Health Records, but also to unsuspicious type of information.

There is a growing concern that these schemes may be implemented in manner which does not always respect the patients' confidentiality and basic rights, and in a broader context, the use of this of information may prejudice the individuals concerned.

The ability to track and monitor patients and resources enables a more efficient provision of care but may have an impact on the right to privacy of the individual concerned.

2.2. Questions: Is your legal framework providing for a regulation of Cloud Computing, Data Mining and Profiling? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	No. No info.
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Cloud computing:	How is cloud computing regulated in your country? Which security safeguards and standards are mandatory? Are there specific requirements in order to store medical data in the cloud? How data is shared and is the sharing regulated?
	Cloud computing for medical data is not regulated in the field where I work (specialization). Protection measures are only firewall and password log in.
Government:	Do governmental programs exist to allow for increased data-mining of medical records? If yes, what are the purposes of this data mining? Are private entities allowed to access the data? Under what circumstances? What sort of techniques and technologies are being used? To what end? Are data subjects informed of this type of data-mining?
	We don't have enough info upon this question.
Private sector:	Are private entities allowed to mine medical data which they process? Under what circumstances? Can the government have access to this data?
	All private medical in institutions have the same access as state medical instutions.
Profiling:	Are the government and the private sector allowed to employ profiling methods on medical data? If yes, under what circumstances? Is it allowed to cross and correlate non-medical data with medical data?
	No info.

3. RFID and wireless communication technologies

3.1. Data Protection Issues:

It is common for medical devices, such as patients' tags, to possess RFID technologies in order to facilitate the transmission of the patients' data.

It can also be related to the data-mining operations previously mentioned as it is another category of information that can be used to discern meaningful patterns.

Transmission of data through radio-frequency is not limited to medical devices. Almost any smartphone uses some technology enabling to collect, and share, the user's data. For instance, via WI-FI it is possible to identify users' locations and therefore infer some of their behaviour, which in some cases can relate to health information.

3.2. Questions: Is your legal framework providing for a regulation of RFID technologies and the transfer of personal data through wireless technologies? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	No info
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
RFID:	How is RFID used in hospital/clinics for (a) resource management, (b) patient care? What types of database systems (and security) are implemented in conjunction with RFID use? How are issues of access, sharing, consent etc. managed considering that RFID may be used without the patients' knowledge.
	We don't have such info.
Wireless tracking technologies:	Are hospitals/clinics employing other wireless tracking technologies besides RFID? Which ones? Do they have to follow specific security requirements? Which ones?
	NO info.

4. Applications (Mobile)

4.1. Data Protection Issues:

Information society is increasingly relying on the use of "apps" (application), most of them mobile. These apps are commonly designed to gather personal data, and in practice often process medical data.
Technologies such as multi-touch touchscreen, accelerometers or gyroscopes, ambient light sensors, GPS and cameras, and devices featuring fingerprint and biometric sensors also involve the collection of medical data.

A mobile phone application can monitor accurately physiological data, such as heartbeats, sleep patterns, fitness information.

4.2. Questions: Is your legal framework providing for a regulation of Apps and Mobile Apps? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	No info
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Apps:	Is it allowed to use apps and mobile apps to deploy medical services and collect medical data? If yes, which type of individual/organisation can develop and employ these apps? Are there specific security requirements for these types of apps?
	No
Institutions:	Do hospitals/clinics/labs employ apps to gather medical data? Is there a need for a medical treatment to permit the use of an app to process the medical data? Are there specific security requirements for the institutions collecting these data from the apps? Are medico-administrative data used by hospitals/clinics for management purposes?
	No info.
Tracking technologies:	Do hospitals/clinics/labs employ non-medical apps and devices to track and collect data from their patients? What type of data is collected? For what purpose? Is the data identifiable? Is the data combined with medical data?
	No info.
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical apps and tracking apps? If yes, what are the standards?
	No info.
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical diagnostic? How would this be applied to fitness and daily-basis data?
	No info.

5. Medical Devices and Wearable Devices

5.1. Data Protection Issues:

A medical device can be defined as: 'any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application. Such a device should be intended by the manufacturer for one of a number of defined purposes, one of which is, diagnosis, prevention, monitoring, treatment or alleviation of disease' (Directive 93/42/EEC Article 1:2)

Some eHealth and mHealth devices and apps do not fall in this definition of medical devices, as can also be the case of a software working in combination with a physical device, for instance a smartphone.

5.2. Questions: Is your legal framework providing for a regulation of Medical Devices? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	No.
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
eHealth and mHealth:	Does the concept of Medical device in your country encompass services and apparels in the realm of eHealth and mHealth? What are the requirements? Should, for instance, the medical device be certified before it can be used?
	NO info.
Apps:	Does the concept of medical devices encompass apps? If yes, is there any regulation applicable to apps that perform medical services? Is there any regulation applicable on apps that track non-medical data that can lead to health information? If yes, what type of data?
	NO info.
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical and/or wearable devices? If yes, what are the standards?
	Log in and firewall.
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical treatment? How would this be applied to fitness and daily-basis data?
	NO info.

6. Internet of Things

6.1. Data Protection Issues:

Internet of things relates to common, ordinary devices that are now, and increasingly, connected to the Internet, such as cars, fridges, ovens, microwaves, etc. All of these devices can provide data that can lead to reveal information concerning one's health. A fridge can easily inform on the type of food stored and thus the diet of an individual. One of the biggest challenges of the Internet of Things is to guarantee the right to privacy and data protection in a world where every device collects, processes, analyses and transmits the data, commonly via wireless technologies.

In the realm of medical data, the issue mainly arises when crossing seemly unrelated data that can lead to health information about an individual.

6.2. Questions: Is your legal framework providing for a regulation of the Internet of Things? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	NO info.
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Security:	What are the security standards that need to be employed by these devices when collecting personal data?
	NO info.
Non-medical devices:	Are non-medical devices allowed to collect medical data, such as heart frequency? Are they allowed to cross medical data with non-medical data?
	NO info.
Privacy by Design:	Is there any requirement to implement privacy by design in the development of connected devices? If yes, what are the standards?
	NO info.

7. Electronic Doctor (online Doctor) and on-line appointments

7.1. Data Protection Issues:

The Doctor listens, talks and assesses the patient online, via a website, app, canal, sometimes including video-conference. Medical data is collected and processed, what are the security requirements and standards followed? Other websites provide for on-line appointments with doctors, which can also involve the processing of medical data.

7.2. Questions: Is your legal framework providing for a regulation of online Medical Treatment and is the on-line appointment system covered by such a framework? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	There are no online medical examinations.
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Medical treatment:	Is it allowed to perform medical treatment via online services? If yes, how should the medical services be provided? Does it have to follow the same requirements of a regular physically-present medical treatment?
	No
Medical data:	How should the data collected via a medical treatment performed online be processed? Are there specific requirements? Which ones?
	No info.

Other comments and technologies
Should you wish to describe any technology, feature or trend that has not been covered by the questionnaire, please feel free to use the space provided below. Where relevant, also indicate recent legislation changes, guidelines and/or case law.

SWITZERLAND / SUISSE - L'ASSOCIATION DES AUTORITÉS CANTONALES DE LA PROTECTION DES DONNÉES (PRIVATIM)

QUESTIONNAIRE

The questionnaire should ideally be completed by data protection authorities, health policy authorities, professional or patient associations as well as healthcare providers: you are invited to share it as widely as possible.

Please send your replies to dataprotection@coe.int no later than 15 December 2014.

1. Mobile Health (mHealth) and Electronic Health Records (EHR)

1.1. Data Protection Issues:

This is perhaps the biggest topic sitting at the intersection of technology and data protection. Mobile health (mHealth) and Electronic Health Records (EHR) are increasingly used in healthcare systems and provisions – it is a trend that needs to be examined.

Related to the EHR, these records are more accurate, cost-effective (in terms of storage) than paper-based notes. The concept of patient controlled/accessed EHR has been implemented in varying degrees in different countries.

Furthermore, some non-medical record can still contain health information about users and it should be considered if such records ought to be treated in a similar way to EHR.

Also, should 'medical data' as defined in Recommendation N° (97) 5 on the protection of medical data cover physical tracking data, such as pedometers or fitness data and data that can lead to medical information about an individual ?

1.2. Questions: if EHR exist in your country, is your legal framework providing for a regulation of such records? If mHealth exists in your country, is your legal framework providing for a specific regulation? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	The cantonal laws and its corresponding regulations (in canton Basel-Stadt for example the law of 9 June 2010 on Information and Data protection [IDPA, SG 153.260] and the IDV [SG 153.270]) contain the *general* data protection legislation. These acts provide the general rules for the processing of special personal data (such as health data): Such processing is only allowed if an act *explicitly* authorizes or requires this or the processing is *absolutely necessary* for a task that is clearly defined in an act. In addition, the processing of personal data must be carried out in good faith and must be proportionate (for example § 9 IDPA). If the data processing is allowed the public body has to protect the data by means of appropriate organizational and technical measures. The measures must be designed to achieve the following protection goals: confidentiality (Information must not fall into unauthorized hands), integrity (must be correct and complete) and availability (must be available when needed). Information processing must be attributable to a specific person an amendments to information must be recognizable and plausible. The measures to be taken depend on the nature of the information, the nature

	«Value») and purpose of use and the current state of technology (for example § 8 IDPA). For example in Basel-Stadt there are plans to start an eHealth pilot project «Regio Basel» with the aim to introduce the electronic Patient File («ePatientendossier»). But until now the necessary legal frameworks have not yet been finalized, so such a data processing is not allowed. If any further information concerning thes project or projects in other cantons is required, please contact the responsible cantonal (Health-) Department.
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
EHR and Medical data:	What can be considered medical data in your country? Is it solely the data relating to a person's health (state, diagnosis, prognosis, medical treatment, etc.)? Is non-medical data that leads to medical information treated the same way as medical data (for instance in terms of confidentiality requirements)? Is the EHR solely constituted of data collected in a medical context or can the individual also himself or herself add information regarding his or her health?
	For example in canton Basel-Stadt there is no special definition of **medical data**. So medical data are generally understood as data relating to a person's health. Nevertheless, through the compilation of not typical medical data medical data can be generated. Such compilations of information that enable the evaluation of crucial aspects of the personality are understood as special personal data (for example § 3 Abs. 4 IDPA), for which count the same provisions as for typical medical data (see 1.2. legislation).
Sharing of data and Access:	Who is granted access to the EHR and how is the sharing of information (with other health care providers?) regulated? Where information is shared with pharmacists, is there a strict purpose limitation in place? How has the definition of the responsibility over the medical data been regulated?
	No reply possible – see answer 1.2 (legislation)
Data quality:	Are the principles of legitimacy, fairness and minimisation applied to medical data? How are records kept accurate? How long is the data kept for, is the specific storage period defined for the EHR?
	The principles of legitimacy, fairness and minimization must be applied to every kind of data. Therefore also to medical data.
Data integrity:	Are any specific methods used to ensure the integrity of the data? How are patients identified in the EHR? In the context of research, are anonymisation methods used and what safeguards exist for re-identification?
	No reply possible – see answer 1.2 (legislation)
Data security:	Where are the records stored? Is there a centralised database of EHR? What security technology is being used?
	No reply possible – see answer 1.2 (legislation)
Rights of the person/patient concerned:	How can the right of access be exercised? How can the data be corrected? Can the person enter information in his or her own EHR? What are the legal remedies available?
	No reply possible – see answer 1.2 (legislation)

Consent:	Is the system based on an opt-in approach? Is the principle of granular consent applied (with the possibility of preventing access to certain data?)? If yes, in which situations?
	No reply possible – see answer 1.2 (legislation)
Withdrawal:	Are patients able to withdraw the consent given to EHR schemes? If yes, what is the relevant procedure to withdraw such consent? What are the consequences?
	No reply possible – see answer 1.2 (legislation)
Outsourcing processing of data:	Is outsourcing common? Under what circumstances? Where is the data outsourced to? What sort of safeguards are in place?
	No reply possible – see answer 1.2 (legislation)

2. Cloud Computing, Data Mining and Profiling from both Medical Records (including EHR) and Data not specifically related to medical records.

2.1. Data Protection Issues:

Cloud computing has brought a new dimension to the way data is stored, accessed and processed. Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS), Network as a service (NaaS) are all used by services and organisations that deal with both medical data and non-medical data.

With the development of more advanced and efficient data-mining and data-querying Medical techniques (e.g NoSQL, MapReduce, Hadoop) in conjunction with increased processing power and data storage, mining data has never been more informative, easier, and cost-effective.

Healthcare is a natural sector in which to apply new technologies and methodologies, with particular impacts in epidemiology, public health, health services research, etc.

Data that can lead to the identification of a particular individual and his/her health situation is not limited to medical data *per se,* present on Electronic Health Records, but also to unsuspicious type of information.

There is a growing concern that these schemes may be implemented in manner which does not always respect the patients' confidentiality and basic rights, and in a broader context, the use of this of information may prejudice the individuals concerned.

The ability to track and monitor patients and resources enables a more efficient provision of care but may have an impact on the right to privacy of the individual concerned.

2.2. Questions: Is your legal framework providing for a regulation of Cloud Computing, Data Mining and Profiling? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	For example in canton Basel-Stadt there is no special legal regulation for **Data Mining**. Therefore, the general regulations are applicable (see 1.2. legislation), what means that without an act that explicitly authorizes the public body to this data processing or that clearly defines a task which the public body can only fulfill with this data processing, the relevant data processing isn't allowed. The principles of data reduction and data economy may also be defined in the cantonal legislations (for example § 14 IDPA). In canton Basel-Stadt there's as well no special legal regulation for **Cloud**

	Computing. Cloud Computing is handled as a case of processing by third parties (§ 7 IDPA), which provides that public bodies may allocate the processing of information to third parties if no legal provision or contractual agreements interdict this and if it is guaranteed that the information is processes only in the same way that he public body would do so. According to law, the public bodies remain responsible for the handling of the respective information. For example § 51 IDPA provides a penalty provision for processing of personal data that is in breach of contract: Any mandated person within the meaning of § 7 IDPA who, without the express authorization of the mandating public body, deliberately or negligently uses personal data for himself or herself or for others or discloses such data will be liable to a fine. **Personal profiles** belong to the special personal data (for example § 3 Abs. 4 IDPA), which enjoy a higher protection standard. But there is no special legislation for Profiling. It is assumed that other cantons handle the topics the same way.
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Cloud computing:	How is cloud computing regulated in your country? Which security safeguards and standards are mandatory? Are there specific requirements in order to store medical data in the cloud? How is data shared and is the sharing regulated?
	See answer above (2.2 legislation)
Government:	Do governmental programmes exist to allow for increased data-mining of medical records? If yes, what are the purposes of this data mining? Are private entities allowed to access the data? Under what circumstances? What sort of techniques and technologies are being used? To what end? Are data subjects informed of this type of data-mining?
	For information please contact the responsible cantonal Department.
Private sector:	Are private entities allowed to mine medical data which they process? Under what circumstances? Can the government have access to this data?
	For information please contact the responsible cantonal Department.
Profiling:	Are the government and the private sector allowed to employ profiling methods on medical data? If yes, under what circumstances? Is it allowed to cross and correlate non-medical data with medical data?
	For information please contact the responsible cantonal Department.

3. RFID and wireless communication technologies

3.1. Data Protection Issues:

It is common for medical devices, such as patients' tags, to possess RFID technologies in order to facilitate the transmission of the patients' data.

It can also be related to the data-mining operations previously mentioned as it is another category of information that can be used to discern meaningful patterns.

Transmission of data through radio-frequency is not limited to medical devices. Almost any smartphone uses some technology enabling to collect, and share, the user's data. For instance, via WI-FI it is possible to identify users' locations and therefore infer some of their behaviour, which in some cases can relate to health information.

3.2. Questions: Is your legal framework providing for a regulation of RFID technologies and the transfer of personal data through wireless technologies? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	As far as we know there is no special regulation of RFID technologies. So the general regulations are applicable (see 1.2. legislation) what means that without an act that explicitly authorizes the public body to this data processing or that clearly defines a task which the public body can only fulfill with this data processing, the relevant data processing isn't allowed. Whatever the data processor is allowed to do, there must be a risk analysis and the hazard for consequences mustn't be too big (impact assessment).
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
RFID:	How is RFID used in hospital/clinics for (a) resource management, (b) patient care? What types of database systems (and security) are implemented in conjunction with RFID use? How are issues of access, sharing, consent etc. managed considering that RFID may be used without the patients' knowledge.
	For information please contact the responsible cantonal Department.
Wireless tracking technologies:	Are hospitals/clinics employing other wireless tracking technologies besides RFID? Which ones? Do they have to follow specific security requirements? Which ones?
	For information please contact the responsible cantonal Department

4. Applications (Mobile)

4.1. Data Protection Issues: Information society is increasingly relying on the use of "apps" (application), most of them mobile. These apps are commonly designed to gather personal data, and in practice often process medical data. Technologies such as multi-touch touchscreen, accelerometers or gyroscopes, ambient light sensors, GPS and cameras, and devices featuring fingerprint and biometric sensors also involve the collection of medical data. A mobile phone application can monitor accurately physiological data, such as heartbeats, sleep patterns, fitness information.

4.2. Questions: Is your legal framework providing for a regulation of Apps and Mobile Apps? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	No, as far as we know there is no special regulation of Apps. So the general regulations are applicable (see 1.2. legislation) what means that without an act that explicitly authorizes the public body to this data processing or that clearly defines a task which the public body can only fulfill with this data processing, the relevant data processing isn't allowed.

Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Apps:	Is it allowed to use apps and mobile apps to deploy medical services and collect medical data? If yes, which type of individual/organisation can develop and employ these apps? Are there specific security requirements for these types of apps?
	For information please contact the responsible cantonal Department.
Institutions:	Do hospitals/clinics/labs employ apps to gather medical data? Is there a need for a medical treatment to permit the use of an app to process the medical data? Are there specific security requirements for the institutions collecting these data from the apps? Are medico-administrative data used by hospitals/clinics for management purposes?
	For information please contact the responsible cantonal Department.
Tracking technologies:	Do hospitals/clinics/labs employ non-medical apps and devices to track and collect data from their patients? What type of data is collected? For what purpose? Is the data identifiable? Is the data combined with medical data?
	For information please contact the responsible cantonal Department.
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical apps and tracking apps? If yes, what are the standards?
	For information please contact the responsible cantonal Department.
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical diagnostic? How would this be applied to fitness and daily-basis data?
	For information please contact the responsible cantonal Department.

5. Medical Devices and Wearable Devices

5.1. Data Protection Issues:

A medical device can be defined as: 'any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application. Such a device should be intended by the manufacturer for one of a number of defined purposes, one of which is, diagnosis, prevention, monitoring, treatment or alleviation of disease' (Directive 93/42/EEC Article 1:2)

Some eHealth and mHealth devices and apps do not fall in this definition of medical devices, as can also be the case of a software working in combination with a physical device, for instance a smartphone.

5.2. Questions: Is your legal framework providing for a regulation of Medical Devices? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	No, as far as we know there is no special regulation of Medical Devices. So the general regulations are applicable (see 1.2. legislation) what means that without an

	act that explicitly authorizes the public body to this data processing or that clearly defines a task which the public body can only fulfill with this data processing, the relevant data processing isn't allowed.
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
eHealth and mHealth:	Does the concept of Medical device in your country encompass services and apparels in the realm of eHealth and mHealth? What are the requirements? Should, for instance, the medical device be certified before it can be used?
	No answer possible.
Apps:	Does the concept of medical devices encompass apps? If yes, is there any regulation applicable to apps that perform medical services? Is there any regulation applicable on apps that track non-medical data that can lead to health information? If yes, what type of data?
	No answer possible.
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical and/or wearable devices? If yes, what are the standards?
	No answer possible.
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical treatment? How would this be applied to fitness and daily-basis data?
	No answer possible.

6. Internet of Things

6.1. Data Protection Issues:

Internet of things relates to common, ordinary devices that are now, and increasingly, connected to the Internet, such as cars, fridges, ovens, microwaves, etc. All of these devices can provide data that can lead to reveal information concerning one's health. A fridge can easily inform on the type of food stored and thus the diet of an individual. One of the biggest challenges of the Internet of Things is to guarantee the right to privacy and data protection in a world where every device collects, processes, analyses and transmits the data, commonly via wireless technologies.

In the realm of medical data, the issue mainly arises when crossing seemly unrelated data that can lead to health information about an individual.

6.2. Questions: Is your legal framework providing for a regulation of the Internet of Things? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	No, as far as we know there is no special regulation of the Internet of Things. So the general regulations are applicable (see 1.2. legislation) what means that without an act that explicitly authorizes the public body to this data processing or that clearly defines a task which the public body can only fulfill with this data processing, the relevant data processing isn't allowed.
Case-law:	

Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Security:	What are the security standards that need to be employed by these devices when collecting personal data?
	No answer possible.
Non-medical devices:	Are non-medical devices allowed to collect medical data, such as heart frequency? Are they allowed to cross medical data with non-medical data?
	No answer possible.
Privacy by Design:	Is there any requirement to implement privacy by design in the development of connected devices? If yes, what are the standards?
	No answer possible.

7. Electronic Doctor (online Doctor) and on-line appointments

7.1. Data Protection Issues:

The Doctor listens, talks and assesses the patient online, via a website, app, canal, sometimes including video-conference. Medical data is collected and processed, what are the security requirements and standards followed? Other websites provide for on-line appointments with doctors, which can also involve the processing of medical data.

7.2. Questions: Is your legal framework providing for a regulation of online Medical Treatment and is the on-line appointment system covered by such a framework? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	As far as we know there are no special regulations of electronic Doctor and online appointments. So the general regulations are applicable (see 1.2. legislation) what means that without an act that explicitly authorizes the public body to this data processing or that clearly defines a task which the public body can only fulfill with this data processing, the relevant data processing isn't allowed.
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Medical treatment:	Is it allowed to perform medical treatment via online services? If yes, how should the medical services be provided? Does it have to follow the same requirements of a regular physically-present medical treatment?
	No answer possible.
Medical data:	How should the data collected via a medical treatment performed online be processed? Are there specific requirements? Which ones?
	No answer possible.

Other comments and technologies
Should you wish to describe any technology, feature or trend that has not been covered by the questionnaire, please feel free to use the space provided below. Where relevant, also indicate recent legislation changes, guidelines and/or case law.

SWITZERLAND /SUISSE - REPLIES / RÉPONSES IG - EHEALTH

1. Mobile Health (mHealth) and Electronic Health Records (EHR)

1.1. Data Protection Issues:

This is perhaps the biggest topic sitting at the intersection of technology and data protection. Mobile health (mHealth) and Electronic Health Records (EHR) are increasingly used in healthcare systems and provisions – it is a trend that needs to be examined.

Related to the EHR, these records are more accurate, cost-effective (in terms of storage) than paper-based notes. The concept of patient controlled/accessed EHR has been implemented in varying degrees in different countries.

Furthermore, some non-medical record can still contain health information about users and it should be considered if such records ought to be treated in a similar way to EHR.

Also, should 'medical data' as defined in Recommendation N° (97) 5 on the protection of medical data cover physical tracking data, such as pedometers or fitness data and data that can lead to medical information about an individual ?

1.2. Questions: if EHR exist in your country, is your legal framework providing for a regulation of such records? If mHealth exists in your country, is your legal framework providing for a specific regulation? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	*In Switzerland an EHR law will be introduced in 2017/18. It does not cover mHealth.* *In general data protection law limits strongly the collection of sensitive personal data. Databases containing such data must be registered at national authority. In case of violation a fine must be payed.*
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).

EHR and Medical data:	What can be considered medical data in your country? Is it solely the data relating to a person's health (state, diagnosis, prognosis, medical treatment, etc.)? Is non-medical data that leads to medical information treated the same way as medical data (for instance in terms of confidentiality requirements)? Is the EHR solely constituted of data collected in a medical context or can the individual also himself or herself add information regarding his or her health?
	The swiss data protection law does not specify medical data itself. Any insightful data that will be collected of a person systematically will be taken under the category of particularly sensitive personal data and falls under specific regulated limitations. E.g. the person must be informed which data has been collected if the person asks for it. All data must be deleted or if not erroneous must be corrected on demand of this person. Any handover of these data to a third party must be agreed by the person itself. It does not make a difference who is adding the data. In the end it is the obligation of the provider holding these data to do this in line with the law. Collection of any data may only be done if the circumstance of usefulness is given.

Sharing of data and Access:	Who is granted access to the EHR and how is the sharing of information (with other health care providers?) regulated? Where information is shared with pharmacists, is there a strict purpose limitation in place? How has the definition of the responsibility over the medical data been regulated?
	In a treatment relation the patient gives his consent for this specific treatment. All necessary health professionals may have access to these treatment specific healthcare data. *The new law for EHR enables to collect medical data from different treatments. In this context the patient has to define which date may be shared with which health professional.*
Data quality:	Are the principles of legitimacy, fairness and minimisation applied to medical data? How are records kept accurate? How long is the data kept for, is the specific storage period defined for the EHR?
	The detailed rules are not yet defined. The idea is to keep relevant data as long as they are useful. E.g. medication data may expire very early whereas immunization data should be kept lifelong
Data integrity:	Are any specific methods used to ensure the integrity of the data? How are patients identified in the EHR? In the context of research, are anonymisation methods used and what safeguards exist for re-identification?
	The rules to ensure the integrity of data are not yet defined. A certification procedure is foreseen to guaranty a certain integrity as well as a high level of security. Strong authentication is foreseen to all users accessing the EHR. *Anonymous analyses of medical data shall be possible the detailed rules for anonymisation or pseudonymisation are not yet defined.*
Data security:	Where are the records stored? Is there a centralised database of EHR? What security technology is being used?
	A nationwide centralized storage is prohibited. EHR data shall be stored decentralized and only linked with specific keys allowing to split off again a datasources without losing all links to stored medical documents *The standards of security are not yet defined.*
Rights of the person/patient concerned:	How can the right of access be exercised? How can the data be corrected? Can the person enter information in his or her own EHR? What are the legal remedies available?
	The rights of access can be exercised via a patient portal/interface where the patient can define his personal access rules to his data. The general swiss data protection law gives the right to any person to have any insightful data deleted or to have erroneous data corrected in any data collection holding insightful data this person. *If the provider does not follow the rules he may be punished by a fine*
Consent:	Is the system based on an opt-in approach? Is the principle of granular consent applied (with the possibility of preventing access to certain data?)? If yes, in which situations?

	The swiss EHR law is based on a opt-in approach. The foreseen consent is based on 3 levels. *1. the person / patient has to agree that he wants to participate the EHR System and allows in general that useful medical data may be collected from all different sources to his EHR. He/she may not opt-out granular sources or different types. But* *2. the person/patient may select a preferred model (restricted, normal, open) which fits his needs (preconfigured set of access rules). In addition* *3. the person/patient can adjust individualy access rights up to document level and/or individual person to whom he/she wants to show or hide documents. Any data may be declared secret (no access for anybody) or stigmatizing (access for a very limited number of persons). In addition the person/patient may declare different data sources where all data must be declared as secret or as stigmatizing to prevent or limit automatically any access to these documents.* *In this system not the collection of documents is limited only accessing documents will be limited by authorization rules.*
Withdrawal:	Are patients able to withdraw the consent given to EHR schemes? If yes, what is the relevant procedure to withdraw such consent? What are the consequences?
	The person/patient may withdraw at any time the access to a specific document or change rules for users accessing the EHR. The patient/person may hide temporally all his documents to any health professional. As the documents are still exist but marked as secret. These documents may be visible again later on if the person decides to grant access again. *If the patient decides to quit his EHR his record must be deleted according the general data protection law.*
Outsourcing processing of data:	Is outsourcing common? Under what circumstances? Where is the data outsourced to? What sort of safeguards are in place?
	Outsourcing is common as long as data is held in Switzerland. As in this case sensitive data are passed to a third party the patient/person must be informed to whom this outsourcing will take place. If any sensitive data is outsourced abroad the person must agree/give his consent to outsource abroad. *The company collecting data is responsible to keep compliant even if the operations are outsourced to another party*

2. Cloud Computing, Data Mining and Profiling from both Medical Records (including EHR) and Data not specifically related to medical records.

2.1. Data Protection Issues:

Cloud computing has brought a new dimension to the way data is stored, accessed and processed. Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS), Network as a service (NaaS) are all used by services and organisations that deal with both medical data and non-medical data.

With the development of more advanced and efficient data-mining and data-querying Medical techniques (e.g NoSQL, MapReduce, Hadoop) in conjunction with increased processing power and data storage, mining data has never been more informative, easier, and cost-effective.

Healthcare is a natural sector in which to apply new technologies and methodologies, with particular impacts in epidemiology, public health, health services research, etc.

Data that can lead to the identification of a particular individual and his/her health situation is not limited to medical data *per se,* present on Electronic Health Records, but also to unsuspicious type of information.

There is a growing concern that these schemes may be implemented in manner which does not always respect the patients' confidentiality and basic rights, and in a broader context, the use of this of information may prejudice the individuals concerned.

The ability to track and monitor patients and resources enables a more efficient provision of care but may have an impact on the right to privacy of the individual concerned.

2.2. Questions: Is your legal framework providing for a regulation of Cloud Computing, Data Mining and Profiling? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	*The general data protection law limits who may work with sensitive data in that manner, that any third party accessing sensitive data must be declared and announced to the person (data owner). Collecting data must in a useful relation to the object why data had been collected for.* *It does not matter how data are processed or stored. In the end the responsible provider collecting data is responsible to be compliant with the general data protection law. If this provider stores data on a third party system, this provider must declare this to all data owners (patients/persons). In addition the provider may be asked to proof that this data collection is safe and compliant to swiss data protection law. This obligation and the difficulty to proof that data in the cloud are safe and proper segregated from access of any third party will today prevent providers to store sensitive data in the cloud*.
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Cloud computing:	How is cloud computing regulated in your country? Which security safeguards and standards are mandatory? Are there specific requirements in order to store medical data in the cloud? How is data shared and is the sharing regulated?
	Cloud computing is not specifically regulated. The general data protection law and its rules are applicable. Storing in the cloud means the same as outsourcing to a third party. The provider which outsources to a third party still is responsible and must be compliant with the data protection law. *If medical or sensitive data are made available for a retrieval process, means that many different persons (health professionals) may access medical or sensitive data in a automated way, a special legal basis /framework must be in place.* *To allow an EHR which makes a collection of medical data available for many different persons (health professionals) the swiss EHR law will be introduced in 2017/18*
Government:	Do governmental programmes exist to allow for increased data-mining of medical records? If yes, what are the purposes of this data mining? Are private entities allowed to access the data? Under what circumstances? What sort of techniques and technologies are being used? To what end? Are data subjects informed of this type of data-mining?

	Switzerland introduced 2014 a new human research act which regulates in detail the circumstances which data may be used for research, the rules for patient consent as well as what for these data may be used.
Private sector:	Are private entities allowed to mine medical data which they process? Under what circumstances? Can the government have access to this data?
	Yes they are allowed to do so if the patient gives his explicit informed consent to work with his genome or if he did not deny explicitly to work with non-genome data. *The government may put the public interest above private interest in given situations (e.g. epidemic) .*
Profiling:	Are the government and the private sector allowed to employ profiling methods on medical data? If yes, under what circumstances? Is it allowed to cross and correlate non-medical data with medical data?
	For medical date see above. As long as non-medical data are not sensitive data, a correlation is allowed.

3. RFID and wireless communication technologies

3.1. Data Protection Issues:

It is common for medical devices, such as patients' tags, to possess RFID technologies in order to facilitate the transmission of the patients' data.

It can also be related to the data-mining operations previously mentioned as it is another category of information that can be used to discern meaningful patterns.

Transmission of data through radio-frequency is not limited to medical devices. Almost any smartphone uses some technology enabling to collect, and share, the user's data. For instance, via WI-FI it is possible to identify users' locations and therefore infer some of their behaviour, which in some cases can relate to health information.

3.2. Questions: Is your legal framework providing for a regulation of RFID technologies and the transfer of personal data through wireless technologies? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	*The general data protection law says that personal data must be protected against access from third party. A transfer of sensitive or personnel data must be protected by adequate encryption if a relation to a specific person may be done*.
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
RFID:	How is RFID used in hospital/clinics for (a) resource management, (b) patient care? What types of database systems (and security) are implemented in conjunction with RFID use? How are issues of access, sharing, consent etc. managed considering that RFID may be used without the patients' knowledge.
	RFID is partially used in hospitals. As long as we know there are no sensitive contents linked to patients. Clinic information systems must be preotected against access from authorized third parties. For these systems the general data protection law is applicable. In addition some cantonal law regulates details how to treat medical data in public hospitals.

Wireless tracking technologies:	Are hospitals/clinics employing other wireless tracking technologies besides RFID? Which ones? Do they have to follow specific security requirements? Which ones?

4. Applications (Mobile)

4.1. Data Protection Issues:

Information society is increasingly relying on the use of "apps" (application), most of them mobile. These apps are commonly designed to gather personal data, and in practice often process medical data.
Technologies such as multi-touch touchscreen, accelerometers or gyroscopes, ambient light sensors, GPS and cameras, and devices featuring fingerprint and biometric sensors also involve the collection of medical data.

A mobile phone application can monitor accurately physiological data, such as heartbeats, sleep patterns, fitness information.

4.2. Questions: Is your legal framework providing for a regulation of Apps and Mobile Apps? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	*For mobile devices the telecommunications act is applicable.*
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Apps:	Is it allowed to use apps and mobile apps to deploy medical services and collect medical data? If yes, which type of individual/organisation can develop and employ these apps? Are there specific security requirements for these types of apps?
	There is no specific regulation to use mobile apps to deploy medical services or collecting data. *In the end the data protection law is applicable if any sensitive data is collected. If sensitive data is collected outside of Switzerland the patient / person has to give his informed consent to every date (opt in) stored to the database.* *In practice most of the apps are not compliant.*
Institutions:	Do hospitals/clinics/labs employ apps to gather medical data? Is there a need for a medical treatment to permit the use of an app to process the medical data? Are there specific security requirements for the institutions collecting these data from the apps? Are medico-administrative data used by hospitals/clinics for management purposes?
	Yes they do. For professional apps the same rules as for other it equipment dealing with medical data are applicable (data protection law, cantonal medical law).
Tracking technologies:	Do hospitals/clinics/labs employ non-medical apps and devices to track and collect data from their patients? What type of data is collected? For what purpose? Is the data identifiable? Is the data combined with medical data?

Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical apps and tracking apps? If yes, what are the standards?
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical diagnostic? How would this be applied to fitness and daily-basis data?
	For apps the same rules as for other it equipment dealing with medical data are applicable (data protection law, cantonal medical law) *If fitness and daily basis data is used for medical purpose same standards are applicable as for medical devices*

5. Medical Devices and Wearable Devices

5.1. Data Protection Issues:

A medical device can be defined as: 'any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application. Such a device should be intended by the manufacturer for one of a number of defined purposes, one of which is, diagnosis, prevention, monitoring, treatment or alleviation of disease' (Directive 93/42/EEC Article 1:2)

Some eHealth and mHealth devices and apps do not fall in this definition of medical devices, as can also be the case of a software working in combination with a physical device, for instance a smartphone.

5.2. Questions: Is your legal framework providing for a regulation of Medical Devices? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	For medical devices the remedies act is applicable
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
eHealth and mHealth:	Does the concept of Medical device in your country encompass services and apparels in the realm of eHealth and mHealth? What are the requirements? Should, for instance, the medical device be certified before it can be used?
	The remedies act covers all medical devices, software and all subjects which are intended to be used to influence positive a treatment. *Medical devices must not harm patients, must work as promised the positive effect of treatment must be evident and provable.*
Apps:	Does the concept of medical devices encompass apps? If yes, is there any regulation applicable to apps that perform medical services? Is there any regulation applicable on apps that track non-medical data that can lead to health information? If yes, what type of data?

	If the device is not intended for medical purpose, it is not a medical device whereas the remedies act is not applicable. If a seller intends to sell the device for medical purpose the remedies act is a applicable. *If non-medical data are used within a promise of a medical treatment and the app is sold for medical purpose the remedies act is applicable and the app will be treated as medical device.*
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical and/or wearable devices? If yes, what are the standards?
	If the device collects sensitive profiles of a person the data protection law or/and the telecommunication act are applicable.
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical treatment? How would this be applied to fitness and daily-basis data?
	It depends for what purpose the seller introduces the product. If the seller positions his product for medical purpose, it falls under the remedies act and will be treated as a medical device, independent of the collected data.

6. Internet of Things

6.1. Data Protection Issues:

Internet of things relates to common, ordinary devices that are now, and increasingly, connected to the Internet, such as cars, fridges, ovens, microwaves, etc. All of these devices can provide data that can lead to reveal information concerning one's health. A fridge can easily inform on the type of food stored and thus the diet of an individual. One of the biggest challenges of the Internet of Things is to guarantee the right to privacy and data protection in a world where every device collects, processes, analyses and transmits the data, commonly via wireless technologies.

In the realm of medical data, the issue mainly arises when crossing seemly unrelated data that can lead to health information about an individual.

6.2. Questions: Is your legal framework providing for a regulation of the Internet of Things? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	*The general data protection law is applicable if any data profiles are built up*
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Security:	What are the security standards that need to be employed by these devices when collecting personal data?
	Not directly specified. An appropriate security standard depending on the confidentiality of the collected data / profile must be achieved. Some minimal standards are defined.

Non-medical devices:	Are non-medical devices allowed to collect medical data, such as heart frequency? Are they allowed to cross medical data with non-medical data?
	Yes it is allowed as long as these devices are not intended to be for medical purpose. It is allowed to cross medical with non-medical data as long as no profile are built-up. If a behavior profile is built up or if collected medical data have an impact on privacy to this person or are linked to a person and a medical result may be interpreted these data become sensitive. On collecting sensitive data the general data protection law is applicable.
Privacy by Design:	Is there any requirement to implement privacy by design in the development of connected devices? If yes, what are the standards?
	It depends in the collected data, the concept privacy by design is not known in swiss regulation.

7. Electronic Doctor (online Doctor) and on-line appointments

7.1. Data Protection Issues:

The Doctor listens, talks and assesses the patient online, via a website, app, canal, sometimes including video-conference. Medical data is collected and processed, what are the security requirements and standards followed? Other websites provide for on-line appointments with doctors, which can also involve the processing of medical data.

7.2. Questions: Is your legal framework providing for a regulation of online Medical Treatment and is the on-line appointment system covered by such a framework? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	The telecommunication act is applicable. If any medical advice or result is produced by a software which is intended for medical purpose the remedies act is applicable as well.
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Medical treatment:	Is it allowed to perform medical treatment via online services? If yes, how should the medical services be provided? Does it have to follow the same requirements of a regular physically-present medical treatment?
	In general a medical treatment is allowed via online service but the health insurances are not allowed to pay for medical services within the regular insurance model.
Medical data:	How should the data collected via a medical treatment performed online be processed? Are there specific requirements? Which ones?
	There are no specific requirements, in general a medical doctor has to document the anamnesis, his decisions and treatments independent if he treats face to face or via online service.

Other comments and technologies
Should you wish to describe any technology, feature or trend that has not been covered by the questionnaire, please feel free to use the space provided below. Where relevant, also indicate recent legislation changes, guidelines and/or case law.

Urs Stromer, Walter Stüdeli, IG eHealth (info@ig-ehealth.ch)

SWITZERLAND / SUISSE – REPLIES / REPONSES PFDPT

1. Mobile Health (mHealth) and Electronic Health Records (EHR)

1.1. Data Protection Issues:

This is perhaps the biggest topic sitting at the intersection of technology and data protection. Mobile health (mHealth) and Electronic Health Records (EHR) are increasingly used in healthcare systems and provisions – it is a trend that needs to be examined.

Related to the EHR, these records are more accurate, cost-effective (in terms of storage) than paper-based notes. The concept of patient controlled/accessed EHR has been implemented in varying degrees in different countries.

Furthermore, some non-medical record can still contain health information about users and it should be considered if such records ought to be treated in a similar way to EHR.

Also, should 'medical data' as defined in Recommendation N° (97) 5 on the protection of medical data cover physical tracking data, such as pedometers or fitness data and data that can lead to medical information about an individual ?

1.2. Questions: if EHR exist in your country, is your legal framework providing for a regulation of such records? If mHealth exists in your country, is your legal framework providing for a specific regulation? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	In Switzerland an EHR law and legal ordinance will be introduced in the next years. The commencement of the acts depends on the political process and cannot be fixed yet on a date
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
EHR and Medical data:	What can be considered medical data in your country? Is it solely the data relating to a person's health (state, diagnosis, prognosis, medical treatment, etc.)? Is non-medical data that leads to medical information treated the same way as medical data (for instance in terms of confidentiality requirements)? Is the EHR solely constituted of data collected in a medical context or can the individual also himself or herself add information regarding his or her health?
	The Federal Act on Data Protection (FADP) defines data on health, the intimate sphere or the racial origin as sensitive personal data. All data which leads to personal medical information must be treated the same way as medical data. Even the relationship between patient and physician can be declared as medical information. The goal is that individuals are free to add information to the EHR.
Sharing of data and Access:	Who is granted access to the EHR and how is the sharing of information (with other health care providers?) regulated? Where information is shared with pharmacists, is there a strict purpose limitation in place? How has the definition of the responsibility over the medical data been regulated?
	The patient must consent to provide medical information to the EHR. And the patient himself grants access to the records to individual and identified health professionals. The responsibility over the medical data has been regulated in FADP and the Criminal Code (professional discretion).

Data quality:	Are the principles of legitimacy, fairness and minimization applied to medical data? How are records kept accurate? How long is the data kept for, is the specific storage period defined for the EHR?
	The principals of legitimacy, fairness, minimization and the purpose of the treatment of personal data are defined in the FADP and must be respected in the handling with the medical data. The max. storage time is declared in cantonal laws and are not unique in Switzerland. This declarations will influence the maximal lifetime in the repositories too.
Data integrity:	Are any specific methods used to ensure the integrity of the data? How are patients identified in the EHR? In the context of research, are anonymisation methods used and what safeguards exist for re-identification?
	The FADP requests to protect data with the actual best technical procedure. The details in ensure integrity of the data is not yet defined. Encryption of the data seems to be adequate to the high sensibility of the data.
Data security:	Where are the records stored? Is there a centralized database of EHR? What security technology is being used?
	EHR data shall be stored decentralized.
Rights of the person/patient concerned:	How can the right of access be exercised? How can the data be corrected? Can the person enter information in his or her own EHR? What are the legal remedies available?
	The right of access can be exercised by the patient via user- (patient-) interface. The original medical documents in primary systems cannot be changed. Any correction leads to a new document. The rights of access can be changed every time by the patient.
Consent:	Is the system based on an opt-in approach? Is the principle of granular consent applied (with the possibility of preventing access to certain data?)? If yes, in which situations?
	In general the privacy protection law demands an opt-in-approach. A granular consent is applied. The basic consent is to participate the eHealth-System. Than the patient can agree to provide medical documents in the EHR. And finally he grant access to a document to a identified person.
Withdrawal:	Are patients able to withdraw the consent given to EHR schemes? If yes, what is the relevant procedure to withdraw such consent? What are the consequences?
	The patient can every time withdraw all the consents he made. This should not lead to a malus for the patient.
Outsourcing processing of data:	Is outsourcing common? Under what circumstances? Where is the data outsourced to? What sort of safeguards are in place?
	Outsourcing in EHealth is quite common. Outsourcing in the EHR project will be a fact. MPIs, registries and - in defined degree – repositories will be centralized services for physicians supplied by a community.

2. Cloud Computing, Data Mining and Profiling from both Medical Records (including EHR) and Data not specifically related to medical records.

2.1. Data Protection Issues:

Cloud computing has brought a new dimension to the way data is stored, accessed and processed. Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS), Network as a service (NaaS) are all used by services and organisations that deal with both medical data and non-medical data.

With the development of more advanced and efficient data-mining and data-querying Medical techniques (e.g NoSQL, MapReduce, Hadoop) in conjunction with increased processing power and data storage, mining data has never been more informative, easier, and cost-effective.

Healthcare is a natural sector in which to apply new technologies and methodologies, with particular impacts in epidemiology, public health, health services research, etc.

Data that can lead to the identification of a particular individual and his/her health situation is not limited to medical data *per se,* present on Electronic Health Records, but also to unsuspicious type of information.

There is a growing concern that these schemes may be implemented in manner which does not always respect the patients' confidentiality and basic rights, and in a broader context, the use of this of information may prejudice the individuals concerned.

The ability to track and monitor patients and resources enables a more efficient provision of care but may have an impact on the right to privacy of the individual concerned.

2.2. Questions: Is your legal framework providing for a regulation of Cloud Computing, Data Mining and Profiling? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	In Switzerland there exist no special law for "Cloud Computing". It is regulated by the valid legislation. All processing of personal data is regulated by FADP. Further details can be regulated in special laws (e.g. Federal Social Insurance Law). Computing personal data in a cloud demands a special attentions to the contracts with the provider. In case the provider is abroad, the provider's country must have an equivalent data protection level than Switzerland.
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Cloud computing:	How is cloud computing regulated in your country? Which security safeguards and standards are mandatory? Are there specific requirements in order to store medical data in the cloud? How is data shared and is the sharing regulated?
	There is no explicit regulation on Cloud Computing.
Government:	Do governmental programs exist to allow for increased data-mining of medical records? If yes, what are the purposes of this data mining? Are private entities allowed to access the data? Under what circumstances? What sort of techniques and technologies are being used? To what end? Are data subjects informed of this type of data-mining?
	Data-mining with anonymous or pseudonymous data is common for statistical analyses. Data-mining in narrow sense with personal medical data by the government is not known.
Private sector:	Are private entities allowed to mine medical data which they process? Under what circumstances? Can the government have access to this data?
	Private entities are allowed to mine medical data. They have to respect the legal conditions, especially the FADP.
Profiling:	Are the government and the private sector allowed to employ profiling methods on medical data? If yes, under what circumstances? Is it allowed to cross and correlate non-medical data with medical data?

	Private entities are allowed to employ profiling methods medical data. They have to respect the legal conditions, especially the FADP.

3. RFID and wireless communication technologies

3.1. Data Protection Issues:

It is common for medical devices, such as patients' tags, to possess RFID technologies in order to facilitate the transmission of the patients' data.

It can also be related to the data-mining operations previously mentioned as it is another category of information that can be used to discern meaningful patterns.

Transmission of data through radio-frequency is not limited to medical devices. Almost any smartphone uses some technology enabling to collect, and share, the user's data. For instance, via WI-FI it is possible to identify users' locations and therefore infer some of their behaviour, which in some cases can relate to health information.

3.2. Questions: Is your legal framework providing for a regulation of RFID technologies and the transfer of personal data through wireless technologies? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	The FADP demands to protect personal data against a non-authorized access.
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
RFID:	How is RFID used in hospital/clinics for (a) resource management, (b) patient care? What types of database systems (and security) are implemented in conjunction with RFID use? How are issues of access, sharing, consent etc. managed considering that RFID may be used without the patients' knowledge.
Wireless tracking technologies:	Are hospitals/clinics employing other wireless tracking technologies besides RFID? Which ones? Do they have to follow specific security requirements? Which ones?

4. Applications (Mobile)

4.1. Data Protection Issues:

Information society is increasingly relying on the use of "apps" (application), most of them mobile. These apps are commonly designed to gather personal data, and in practice often process medical data.
Technologies such as multi-touch touchscreen, accelerometers or gyroscopes, ambient light sensors, GPS and cameras, and devices featuring fingerprint and biometric sensors also involve the collection of medical data.

A mobile phone application can monitor accurately physiological data, such as heartbeats, sleep patterns, fitness information.

4.2. Questions: Is your legal framework providing for a regulation of Apps and Mobile Apps? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	The FADP and the Telecommunications Act
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Apps:	Is it allowed to use apps and mobile apps to deploy medical services and collect medical data? If yes, which type of individual/organisation can develop and employ these apps? Are there specific security requirements for these types of apps?
	The government has till now no statutory basis to collect medical data with mobile apps. The private sector is allowed to do so with the respect to the FADP. In the national EHR project a certified device could be allowed to send data, verified by a specified health professional, to the EHR. In a private sector also non verified data could be stored.
Institutions:	Do hospitals/clinics/labs employ apps to gather medical data? Is there a need for a medical treatment to permit the use of an app to process the medical data? Are there specific security requirements for the institutions collecting these data from the apps? Are medico-administrative data used by hospitals/clinics for management purposes?
Tracking technologies:	Do hospitals/clinics/labs employ non-medical apps and devices to track and collect data from their patients? What type of data is collected? For what purpose? Is the data identifiable? Is the data combined with medical data?
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical apps and tracking apps? If yes, what are the standards?
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical diagnostic? How would this be applied to fitness and daily-basis data?

5. Medical Devices and Wearable Devices

5.1. Data Protection Issues:

A medical device can be defined as: 'any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application. Such a device should be intended by the manufacturer for one of a number of defined purposes, one of which is, diagnosis, prevention, monitoring, treatment or alleviation of disease' (Directive 93/42/EEC Article 1:2)

Some eHealth and mHealth devices and apps do not fall in this definition of medical devices, as can also be the case of a software working in combination with a physical device, for instance a smartphone.

5.2. Questions: Is your legal framework providing for a regulation of Medical Devices? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	FADP, Federal Social Insurance Law, Medizinprodukteverordnung
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
eHealth and mHealth:	Does the concept of Medical device in your country encompass services and apparels in the realm of eHealth and mHealth? What are the requirements? Should, for instance, the medical device be certified before it can be used?
	The actual version of eHealth doesn't explicitly specify medical devices. A medical device that supports the medical treatment should be certified.
Apps:	Does the concept of medical devices encompass apps? If yes, is there any regulation applicable to apps that perform medical services? Is there any regulation applicable on apps that track non-medical data that can lead to health information? If yes, what type of data?
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical and/or wearable devices? If yes, what are the standards?
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical treatment? How would this be applied to fitness and daily-basis data?
	The eHealth system will be based on an opt-in approach. The reference to a medical treatment is not necessary. But the data must be labeled as qualified (certified device) or nonqualified (consumer device).

6. Internet of Things

6.1. Data Protection Issues:

Internet of things relates to common, ordinary devices that are now, and increasingly, connected to the Internet, such as cars, fridges, ovens, microwaves, etc. All of these devices can provide data that can lead to reveal information concerning one's health. A fridge can easily inform on the type of food stored and thus the diet of an individual. One of the biggest challenges of the Internet of Things is to guarantee the right to privacy and data protection in a world where every device collects, processes, analyses and transmits the data, commonly via wireless technologies.

In the realm of medical data, the issue mainly arises when crossing seemly unrelated data that can lead to health information about an individual.

6.2. Questions: Is your legal framework providing for a regulation of the Internet of Things? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	No. The FADP regulates the data processing in all. The owner of the data collection is focused in the law. The instrument he used to collect the data is not defined. He is obliged to protect the process with actual best technical possibility.
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Security:	What are the security standards that need to be employed by these devices when collecting personal data?
	Collection based on opt-in, full transparency, encrypted storage and transport,
Non-medical devices:	Are non-medical devices allowed to collect medical data, such as heart frequency? Are they allowed to cross medical data with non-medical data?
	They are allowed to. The use of the data in health treatment will be problematic when the content is not verified. So the data must be labeld as not verified.
Privacy by Design:	Is there any requirement to implement privacy by design in the development of connected devices? If yes, what are the standards?

7. Electronic Doctor (online Doctor) and on-line appointments

7.1. Data Protection Issues:

The Doctor listens, talks and assesses the patient online, via a website, app, canal, sometimes including video-conference. Medical data is collected and processed, what are the security requirements and standards followed? Other websites provide for on-line appointments with doctors, which can also involve the processing of medical data.

7.2. Questions: Is your legal framework providing for a regulation of online Medical Treatment and is the on-line appointment system covered by such a framework? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	The telecommunication act is applicable. If any medical advice or result is produced by a software which is intended for medical purpose the remedies act is applicable as well.
Case-law:	The FADP, the Federal Social Insurance Law, cantonal Health Laws and the Criminal Code regulate this processes.
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Medical treatment:	Is it allowed to perform medical treatment via online services? If yes, how should the medical services be provided? Does it have to follow the same requirements of a regular physically-present medical treatment?
	An online medical treatment must be transparent for the patient. He must know who will get knowledge of the fact and the content of the treatment. The link and storage of all information must be enciphered.
Medical data:	How should the data collected via a medical treatment performed online be processed? Are there specific requirements? Which ones?
	The storage of medical data must be enciphered. The company and the place of storage must be transparent to the patient.

Other comments and technologies
Should you wish to describe any technology, feature or trend that has not been covered by the questionnaire, please feel free to use the space provided below. Where relevant, also indicate recent legislation changes, guidelines and/or case law.

SWITZERLAND / SUISSE

The questionnaire should ideally be completed by data protection authorities, health policy authorities, professional or patient associations as well as healthcare providers: you are invited to share it as widely as possible.

Please send your replies to dataprotection@coe.int no later than 15 December 2014.

1. Mobile Health (mHealth) and Electronic Health Records (EHR)

1.1. Data Protection Issues:

This is perhaps the biggest topic sitting at the intersection of technology and data protection. Mobile health (mHealth) and Electronic Health Records (EHR) are increasingly used in healthcare systems and provisions – it is a trend that needs to be examined.

Related to the EHR, these records are more accurate, cost-effective (in terms of storage) than paper-based notes. The concept of patient controlled/accessed EHR has been implemented in varying degrees in different countries.

Furthermore, some non-medical record can still contain health information about users and it should be considered if such records ought to be treated in a similar way to EHR.

Also, should 'medical data' as defined in Recommendation N° (97) 5 on the protection of medical data cover physical tracking data, such as pedometers or fitness data and data that can lead to medical information about an individual ?

1.2. Questions: if EHR exist in your country, is your legal framework providing for a regulation of such records? If mHealth exists in your country, is your legal framework providing for a specific regulation? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	A federal law concerning the electronic health record is currently discussed in the swiss parliament.
Case-law:	None
Other:	None

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
EHR and Medical data:	What can be considered medical data in your country? Is it solely the data relating to a person's health (state, diagnosis, prognosis, medical treatment, etc.)? Is non-medical data that leads to medical information treated the same way as medical data (for instance in terms of confidentiality requirements)? Is the EHR solely constituted of data collected in a medical context or can the individual also himself or herself add information regarding his or her health?
	In Switzerland, the cantons are mainly responsible for healthcare. Therefore, they define what can be considered medical data.
Sharing of data and Access:	Who is granted access to the EHR and how is the sharing of information (with other health care providers?) regulated? Where information is shared with pharmacists, is there a strict purpose limitation in place? How has the definition of the responsibility over the medical data been regulated?
	Currently, there's no legislation on the EHR. The principles of the law in data protection (DSG; SR 235.1: http://www.admin.ch/opc/de/classified-compilation/19920153/index.html) are applicable for pilot projects.

Data quality:	Are the principles of legitimacy, fairness and minimisation applied to medical data? How are records kept accurate? How long is the data kept for, is the specific storage period defined for the EHR?
	In Switzerland, the cantons are mainly responsible for healthcare. Therefore, they are responsible for these regulations.
Data integrity:	Are any specific methods used to ensure the integrity of the data? How are patients identified in the EHR? In the context of research, are anonymisation methods used and what safeguards exist for re-identification?
	In Switzerland, the cantons are mainly responsible for healthcare. Therefore, they are responsible for these regulations.
Data security:	Where are the records stored? Is there a centralised database of EHR? What security technology is being used?
	In Switzerland, the cantons are mainly responsible for healthcare. Therefore, they are responsible for these regulations.
Rights of the person/patient concerned:	How can the right of access be exercised? How can the data be corrected? Can the person enter information in his or her own EHR? What are the legal remedies available?
	Currently, there's no legislation on the EHR. The principles of the law in data protection (DSG; SR 235.1: http://www.admin.ch/opc/de/classified-compilation/19920153/index.html) are applicable for pilot projects.
Consent:	Is the system based on an opt-in approach? Is the principle of granular consent applied (with the possibility of preventing access to certain data?)? If yes, in which situations?
	Currently, there's no legislation on the EHR. A federal law concerning the electronic health record with an opt-in approach is currently discussed in the swiss parliament. The principles of the law in data protection (DSG; SR 235.1: http://www.admin.ch/opc/de/classified-compilation/19920153/index.html) are applicable for pilot projects.
Withdrawal:	Are patients able to withdraw the consent given to EHR schemes? If yes, what is the relevant procedure to withdraw such consent? What are the consequences?
	Currently, there's no legislation on the EHR. A federal law concerning the electronic health record is currently discussed in the swiss parliament. According to this law, the patient is able to withdraw the consent. He shall not be penalised for such a withdrawl.
Outsourcing processing of data:	Is outsourcing common? Under what circumstances? Where is the data outsourced to? What sort of safeguards are in place?
	In Switzerland, the cantons are mainly responsible for healthcare. Therefore, they are responsible for these regulations.

2. Cloud Computing, Data Mining and Profiling from both Medical Records (including EHR) and Data not specifically related to medical records.

2.1. Data Protection Issues:

Cloud computing has brought a new dimension to the way data is stored, accessed and processed. Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS), Network as a service (NaaS) are all used by services and organisations that deal with both medical data and non-medical data.

With the development of more advanced and efficient data-mining and data-querying Medical techniques (e.g NoSQL, MapReduce, Hadoop) in conjunction with increased processing power and data storage, mining data has never been more informative, easier, and cost-effective. Healthcare is a natural sector in which to apply new technologies and methodologies, with particular impacts in epidemiology, public health, health services research, etc. Data that can lead to the identification of a particular individual and his/her health situation is not limited to medical data *per se,* present on Electronic Health Records, but also to unsuspicious type of information. There is a growing concern that these schemes may be implemented in manner which does not always respect the patients' confidentiality and basic rights, and in a broader context, the use of this of information may prejudice the individuals concerned. The ability to track and monitor patients and resources enables a more efficient provision of care but may have an impact on the right to privacy of the individual concerned.

2.2. Questions: Is your legal framework providing for a regulation of Cloud Computing, Data Mining and Profiling? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	The principles of the law in data protection (DSG; SR 235.1: http://www.admin.ch/opc/de/classified-compilation/19920153/index.html) are applicable for cloud computing. There is no special regulation for cloud computing.
Case-law:	None
Other:	None

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Cloud computing:	How is cloud computing regulated in your country? Which security safeguards and standards are mandatory? Are there specific requirements in order to store medical data in the cloud? How is data shared and is the sharing regulated?
	The principles of the law in data protection (DSG; SR 235.1: http://www.admin.ch/opc/de/classified-compilation/19920153/index.html) are applicable for cloud computing. There is no special regulation for cloud computing.
Government:	Do governmental programmes exist to allow for increased data-mining of medical records? If yes, what are the purposes of this data mining? Are private entities allowed to access the data? Under what circumstances? What sort of techniques and technologies are being used? To what end? Are data subjects informed of this type of data-mining?
	The principles of the law in data protection (DSG; SR 235.1: http://www.admin.ch/opc/de/classified-compilation/19920153/index.html) are applicable for data mining.
Private sector:	Are private entities allowed to mine medical data which they process? Under what circumstances? Can the government have access to this data?
	The principles of the law in data protection (DSG; SR 235.1: http://www.admin.ch/opc/de/classified-compilation/19920153/index.html) are applicable for data mining.
Profiling:	Are the government and the private sector allowed to employ profiling methods on medical data? If yes, under what circumstances? Is it allowed to cross and correlate non-medical data with medical data?
	The principles of the law in data protection (DSG; SR 235.1: http://www.admin.ch/opc/de/classified-compilation/19920153/index.html) are applicable for data mining.

3. RFID and wireless communication technologies

3.1. Data Protection Issues:

It is common for medical devices, such as patients' tags, to possess RFID technologies in order to facilitate the transmission of the patients' data.

It can also be related to the data-mining operations previously mentioned as it is another category of information that can be used to discern meaningful patterns.

Transmission of data through radio-frequency is not limited to medical devices. Almost any smartphone uses some technology enabling to collect, and share, the user's data. For instance, via WI-FI it is possible to identify users' locations and therefore infer some of their behaviour, which in some cases can relate to health information.

3.2. Questions: Is your legal framework providing for a regulation of RFID technologies and the transfer of personal data through wireless technologies? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	The principles of the law in data protection (DSG; SR 235.1: http://www.admin.ch/opc/de/classified-compilation/19920153/index.html) are applicable on RFID principles. But there is no special legislation on RFID.
Case-law:	None
Other:	None

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
RFID:	How is RFID used in hospital/clinics for (a) resource management, (b) patient care? What types of database systems (and security) are implemented in conjunction with RFID use? How are issues of access, sharing, consent etc. managed considering that RFID may be used without the patients' knowledge.
	In Switzerland, the cantons are mainly responsible for healthcare. Therefore, they are responsible for these regulations.
Wireless tracking technologies:	Are hospitals/clinics employing other wireless tracking technologies besides RFID? Which ones? Do they have to follow specific security requirements? Which ones?
	In Switzerland, the cantons are mainly responsible for healthcare. Therefore, they are responsible for these regulations.

4. Applications (Mobile)

4.1. Data Protection Issues:

Information society is increasingly relying on the use of "apps" (application), most of them mobile. These apps are commonly designed to gather personal data, and in practice often process medical data.
Technologies such as multi-touch touchscreen, accelerometers or gyroscopes, ambient light sensors, GPS and cameras, and devices featuring fingerprint and biometric sensors also involve the collection of medical data.

A mobile phone application can monitor accurately physiological data, such as heartbeats, sleep patterns, fitness information.

4.2. Questions: Is your legal framework providing for a regulation of Apps and Mobile Apps? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	The principles of the law in data protection (DSG; SR 235.1: http://www.admin.ch/opc/de/classified-compilation/19920153/index.html) are applicable for mobile apps. But there is no special legislation for them.
Case-law:	None
Other:	None

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Apps:	Is it allowed to use apps and mobile apps to deploy medical services and collect medical data? If yes, which type of individual/organisation can develop and employ these apps? Are there specific security requirements for these types of apps?
	The principles of the law in data protection (DSG; SR 235.1: http://www.admin.ch/opc/de/classified-compilation/19920153/index.html) are applicable for mobile apps. But there is no special legislation for them. In Switzerland, the cantons are mainly responsible for healthcare. Therefore, they are responsible for these regulations.
Institutions:	Do hospitals/clinics/labs employ apps to gather medical data? Is there a need for a medical treatment to permit the use of an app to process the medical data? Are there specific security requirements for the institutions collecting these data from the apps? Are medico-administrative data used by hospitals/clinics for management purposes?
	In Switzerland, the cantons are mainly responsible for healthcare. Therefore, they are responsible for these regulations.
Tracking technologies:	Do hospitals/clinics/labs employ non-medical apps and devices to track and collect data from their patients? What type of data is collected? For what purpose? Is the data identifiable? Is the data combined with medical data?
	In Switzerland, the cantons are mainly responsible for healthcare. Therefore, they are responsible for these regulations.
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical apps and tracking apps? If yes, what are the standards?
	In Switzerland, the cantons are mainly responsible for healthcare. Therefore, they are responsible for these regulations.
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical diagnostic? How would this be applied to fitness and daily-basis data?
	In Switzerland, the cantons are mainly responsible for healthcare. Therefore, they are responsible for these regulations.

5. Medical Devices and Wearable Devices

5.1. Data Protection Issues:

A medical device can be defined as: 'any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application. Such a device should be intended by the manufacturer for one of a number of defined purposes, one of which is, diagnosis, prevention, monitoring, treatment or alleviation of disease' (Directive 93/42/EEC Article 1:2)

Some eHealth and mHealth devices and apps do not fall in this definition of medical devices, as can also be the case of a software working in combination with a physical device, for instance a smartphone.

5.2. Questions: Is your legal framework providing for a regulation of Medical Devices? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	We have an act on medical devices (Medizinalproduktverordnung, MepV; SR 812.213; http://www.admin.ch/opc/de/classified-compilation/19995459/index.html)
Case-law:	See www.bger.ch
Other:	None

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
eHealth and mHealth:	Does the concept of Medical device in your country encompass services and apparels in the realm of eHealth and mHealth? What are the requirements? Should, for instance, the medical device be certified before it can be used?
	These problems are currently being discussed.
Apps:	Does the concept of medical devices encompass apps? If yes, is there any regulation applicable to apps that perform medical services? Is there any regulation applicable on apps that track non-medical data that can lead to health information? If yes, what type of data?
	These problems are currently being discussed.
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical and/or wearable devices? If yes, what are the standards?
	These problems are currently being discussed.
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical treatment? How would this be applied to fitness and daily-basis data?
	These problems are currently being discussed.

6. Internet of Things

6.1. Data Protection Issues:

Internet of things relates to common, ordinary devices that are now, and increasingly, connected to the Internet, such as cars, fridges, ovens, microwaves, etc. All of these devices can provide data that can lead to reveal information concerning one's health. A fridge can easily inform on the type of food stored and thus the diet of an individual. One of the biggest challenges of the Internet of Things is to guarantee the right to privacy and data protection in a world where every device collects, processes, analyses and transmits the data, commonly via wireless technologies.

In the realm of medical data, the issue mainly arises when crossing seemly unrelated data that can lead to health information about an individual.

6.2. Questions: Is your legal framework providing for a regulation of the Internet of Things? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	The principles of the law in data protection (DSG; SR 235.1: http://www.admin.ch/opc/de/classified-compilation/19920153/index.html) are applicable. But there is no special legislation.
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Security:	What are the security standards that need to be employed by these devices when collecting personal data?
	The principles of the law in data protection (DSG; SR 235.1: http://www.admin.ch/opc/de/classified-compilation/19920153/index.html) are applicable. But there is no special legislation.
Non-medical devices:	Are non-medical devices allowed to collect medical data, such as heart frequency? Are they allowed to cross medical data with non-medical data?
	The principles of the law in data protection (DSG; SR 235.1: http://www.admin.ch/opc/de/classified-compilation/19920153/index.html) are applicable. But there is no special legislation.
Privacy by Design:	Is there any requirement to implement privacy by design in the development of connected devices? If yes, what are the standards?
	The principles of the law in data protection (DSG; SR 235.1: http://www.admin.ch/opc/de/classified-compilation/19920153/index.html) are applicable. But there is no special legislation.

7. Electronic Doctor (online Doctor) and on-line appointments

7.1. Data Protection Issues:

The Doctor listens, talks and assesses the patient online, via a website, app, canal, sometimes including video-conference. Medical data is collected and processed, what are the security requirements and standards followed? Other websites provide for on-line appointments with doctors, which can also involve the processing of medical data.

7.2. Questions: Is your legal framework providing for a regulation of online Medical Treatment and is the on-line appointment system covered by such a framework? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	In Switzerland, the cantons are mainly responsible for healthcare. Therefore, they are responsible for these regulations.
Case-law:	see www.bger.ch
Other:	None

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Medical treatment:	Is it allowed to perform medical treatment via online services? If yes, how should the medical services be provided? Does it have to follow the same requirements of a regular physically-present medical treatment?
	In Switzerland, the cantons are mainly responsible for healthcare. Therefore, they are responsible for these regulations.
Medical data:	How should the data collected via a medical treatment performed online be processed? Are there specific requirements? Which ones?
	In Switzerland, the cantons are mainly responsible for healthcare. Therefore, they are responsible for these regulations.

Other comments and technologies
Should you wish to describe any technology, feature or trend that has not been covered by the questionnaire, please feel free to use the space provided below. Where relevant, also indicate recent legislation changes, guidelines and/or case law.
None

SWITZERLAND / SUISSE - OFFICE FEDERAL DE LA SANTE PUBLIQUE

QUESTIONNAIRE

The questionnaire should ideally be completed by data protection authorities, health policy authorities, professional or patient associations as well as healthcare providers: you are invited to share it as widely as possible.

Please send your replies to dataprotection@coe.int no later than 15 December 2014.

1. Mobile Health (mHealth) and Electronic Health Records (EHR)

1.1. Data Protection Issues:

This is perhaps the biggest topic sitting at the intersection of technology and data protection. Mobile health (mHealth) and Electronic Health Records (EHR) are increasingly used in healthcare systems and provisions – it is a trend that needs to be examined.

Related to the EHR, these records are more accurate, cost-effective (in terms of storage) than paper-based notes. The concept of patient controlled/accessed EHR has been implemented in varying degrees in different countries.

Furthermore, some non-medical record can still contain health information about users and it should be considered if such records ought to be treated in a similar way to EHR.

Also, should 'medical data' as defined in Recommendation N° (97) 5 on the protection of medical data cover physical tracking data, such as pedometers or fitness data and data that can lead to medical information about an individual ?

1.2. Questions: if EHR exist in your country, is your legal framework providing for a regulation of such records? If mHealth exists in your country, is your legal framework providing for a specific regulation? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	*In Switzerland an EHR law will be introduced in 2017/18. It does not cover mHealth.* *In general data protection law limits strongly the collection of sensitive personal data. Databases containing such data must be registered at national authority. In case of violation a fine must be payed.*
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
EHR and Medical data:	What can be considered medical data in your country? Is it solely the data relating to a person's health (state, diagnosis, prognosis, medical treatment, etc.)? Is non-medical data that leads to medical information treated the same way as medical data (for instance in terms of confidentiality requirements)? Is the EHR solely constituted of data collected in a medical context or can the individual also himself or herself add information regarding his or her health?
	The swiss data protection law does not specify medical data itself. Any insightful data that will be collected of a person systematically will be taken under the category of particularly sensitive personal data and falls under specific regulated limitations. E.g. the person must be informed which data has been collected if the

	person asks for it. All data must be deleted or if not erroneous must be corrected on demand of this person. Any handover of these data to a third party must be agreed by the person itself. It does not make a difference who is adding the data. In the end it is the obligation of the provider holding these data to do this in line with the law. Collection of any data may only be done if the circumstance of usefulness is given.
Sharing of data and Access:	Who is granted access to the EHR and how is the sharing of information (with other health care providers?) regulated? Where information is shared with pharmacists, is there a strict purpose limitation in place? How has the definition of the responsibility over the medical data been regulated?
	In a treatment relation the patient gives his consent for this specific treatment. All necessary health professionals may have access to these treatment specific healthcare data. *The new law for EHR enables to collect medical data from different treatments. In this context the patient has to define which date may be shared with which health professional.*
Data quality:	Are the principles of legitimacy, fairness and minimisation applied to medical data? How are records kept accurate? How long is the data kept for, is the specific storage period defined for the EHR?
	The detailed rules are not yet defined. The idea is to keep relevant data as long as they are useful. E.g. medication data may expire very early whereas immunization data should be kept lifelong
Data integrity:	Are any specific methods used to ensure the integrity of the data? How are patients identified in the EHR? In the context of research, are anonymisation methods used and what safeguards exist for re-identification?
	The rules to ensure the integrity of data are not yet defined. A certification procedure is foreseen to guaranty a certain integrity as well as a high level of security. Strong authentication is foreseen to all users accessing the EHR. *Anonymous analyses of medical data shall be possible the detailed rules for anonymisation or pseudonymisation are not yet defined.*
Data security:	Where are the records stored? Is there a centralised database of EHR? What security technology is being used?
	A nationwide centralized storage is prohibited. EHR data shall be stored decentralized and only linked with specific keys allowing to split off again a datasources without losing all links to stored medical documents *The standards of security are not yet defined.*
Rights of the person/patient concerned:	How can the right of access be exercised? How can the data be corrected? Can the person enter information in his or her own EHR? What are the legal remedies available?
	The rights of access can be exercised via a patient portal/interface where the patient can define his personal access rules to his data. The general swiss data protection law gives the right to any person to have any insightful data deleted or to have erroneous data corrected in any data collection holding insightful data this person.

	If the provider does not follow the rules he may be punished by a fine
Consent:	Is the system based on an opt-in approach? Is the principle of granular consent applied (with the possibility of preventing access to certain data?)? If yes, in which situations?
	The swiss EHR law is based on a opt-in approach. The foreseen consent is based on 3 levels. *1. the person / patient has to agree that he wants to participate the EHR System and allows in general that useful medical data may be collected from all different sources to his EHR. He/she may not opt-out granular sources or different types. But* *2. the person/patient may select a preferred model (restricted, normal, open) which fits his needs (preconfigured set of access rules). In addition* *3. the person/patient can adjust individualy access rights up to document level and/or individual person to whom he/she wants to show or hide documents. Any data may be declared secret (no access for anybody) or stigmatizing (access for a very limited number of persons). In addition the person/patient may declare different data sources where all data must be declared as secret or as stigmatizing to prevent or limit automatically any access to these documents.* *In this system not the collection of documents is limited only accessing documents will be limited by authorization rules.*
Withdrawal:	Are patients able to withdraw the consent given to EHR schemes? If yes, what is the relevant procedure to withdraw such consent? What are the consequences?
	The person/patient may withdraw at any time the access to a specific document or change rules for users accessing the EHR. The patient/person may hide temporally all his documents to any health professional. As the documents are still exist but marked as secret. These documents may be visible again later on if the person decides to grant access again. *If the patient decides to quit his EHR his record must be deleted according the general data protection law.*
Outsourcing processing of data:	Is outsourcing common? Under what circumstances? Where is the data outsourced to? What sort of safeguards are in place?
	Outsourcing is common as long as data is held in Switzerland. As in this case sensitive data are passed to a third party the patient/person must be informed to whom this outsourcing will take place. If any sensitive data is outsourced abroad the person must agree/give his consent to outsource abroad. *The company collecting data is responsible to keep compliant even if the operations are outsourced to another party*

2. Cloud Computing, Data Mining and Profiling from both Medical Records (including EHR) and Data not specifically related to medical records.

2.1. Data Protection Issues:

Cloud computing has brought a new dimension to the way data is stored, accessed and processed. Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS), Network as a service (NaaS) are all used by services and organisations that deal with both medical data and non-medical data.

With the development of more advanced and efficient data-mining and data-querying Medical techniques (e.g NoSQL, MapReduce, Hadoop) in conjunction with increased processing power and data storage, mining data has never been more informative, easier, and cost-effective.

Healthcare is a natural sector in which to apply new technologies and methodologies, with particular impacts in epidemiology, public health, health services research, etc.

Data that can lead to the identification of a particular individual and his/her health situation is not limited to medical data *per se,* present on Electronic Health Records, but also to unsuspicious type of information.

There is a growing concern that these schemes may be implemented in manner which does not always respect the patients' confidentiality and basic rights, and in a broader context, the use of this of information may prejudice the individuals concerned.

The ability to track and monitor patients and resources enables a more efficient provision of care but may have an impact on the right to privacy of the individual concerned.

2.2. Questions: Is your legal framework providing for a regulation of Cloud Computing, Data Mining and Profiling? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	*The general data protection law limits who may work with sensitive data in that manner, that any third party accessing sensitive data must be declared and announced to the person (data owner). Collecting data must in a useful relation to the object why data had been collected for.* *It does not matter how data are processed or stored. In the end the responsible provider collecting data is responsible to be compliant with the general data protection law. If this provider stores data on a third party system, this provider must declare this to all data owners (patients/persons). In addition the provider may be asked to proof that this data collection is safe and compliant to swiss data protection law. This obligation and the difficulty to proof that data in the cloud are safe and proper segregated from access of any third party will today prevent providers to store sensitive data in the cloud*.
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Cloud computing:	How is cloud computing regulated in your country? Which security safeguards and standards are mandatory? Are there specific requirements in order to store medical data in the cloud? How is data shared and is the sharing regulated?
	Cloud computing is not specifically regulated. The general data protection law and its rules are applicable. Storing in the cloud means the same as outsourcing to a third party. The provider which outsources to a third party still is responsible and must be compliant with the data protection law. *If medical or sensitive data are made available for a retrieval process, means that many different persons (health professionals) may access medical or sensitive data in a automated way, a special legal basis /framework must be in place.* *To allow an EHR which makes a collection of medical data available for many different persons (health professionals) the swiss EHR law will be introduced in 2017/18*

Government:	Do governmental programmes exist to allow for increased data-mining of medical records? If yes, what are the purposes of this data mining? Are private entities allowed to access the data? Under what circumstances? What sort of techniques and technologies are being used? To what end? Are data subjects informed of this type of data-mining?
	Switzerland introduced 2014 a new human research act which regulates in detail the circumstances which data may be used for research, the rules for patient consent as well as what for these data may be used.
Private sector:	Are private entities allowed to mine medical data which they process? Under what circumstances? Can the government have access to this data?
	Yes they are allowed to do so if the patient gives his explicit informed consent to work with his genome or if he did not deny explicitly to work with non-genome data. *The government may put the public interest above private interest in given situations (e.g. epidemic) .*
Profiling:	Are the government and the private sector allowed to employ profiling methods on medical data? If yes, under what circumstances? Is it allowed to cross and correlate non-medical data with medical data?
	For medical date see above. As long as non-medical data are not sensitive data, a correlation is allowed.

3. RFID and wireless communication technologies

3.1. Data Protection Issues:

It is common for medical devices, such as patients' tags, to possess RFID technologies in order to facilitate the transmission of the patients' data.

It can also be related to the data-mining operations previously mentioned as it is another category of information that can be used to discern meaningful patterns.

Transmission of data through radio-frequency is not limited to medical devices. Almost any smartphone uses some technology enabling to collect, and share, the user's data. For instance, via WI-FI it is possible to identify users' locations and therefore infer some of their behaviour, which in some cases can relate to health information.

3.2. Questions: Is your legal framework providing for a regulation of RFID technologies and the transfer of personal data through wireless technologies? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	*The general data protection law says that personal data must be protected against access from third party. A transfer of sensitive or personnel data must be protected by adequate encryption if a relation to a specific person may be done*.
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
RFID:	How is RFID used in hospital/clinics for (a) resource management, (b) patient care? What types of database systems (and security) are implemented in conjunction with RFID use? How are issues of access, sharing, consent etc. managed considering that RFID may be used without the patients' knowledge.

	RFID is partially used in hospitals. As long as we know there are no sensitive contents linked to patients. Clinic information systems must be preotected against access from authorized third parties. For these systems the general data protection law is applicable. In addition some cantonal law regulates details how to treat medical data in public hospitals.
Wireless tracking technologies:	Are hospitals/clinics employing other wireless tracking technologies besides RFID? Which ones? Do they have to follow specific security requirements? Which ones?

4. Applications (Mobile)

4.1. Data Protection Issues:

Information society is increasingly relying on the use of "apps" (application), most of them mobile. These apps are commonly designed to gather personal data, and in practice often process medical data.
Technologies such as multi-touch touchscreen, accelerometers or gyroscopes, ambient light sensors, GPS and cameras, and devices featuring fingerprint and biometric sensors also involve the collection of medical data.

A mobile phone application can monitor accurately physiological data, such as heartbeats, sleep patterns, fitness information.

4.2. Questions: Is your legal framework providing for a regulation of Apps and Mobile Apps? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	*For mobile devices the telecommunications act is applicable.*
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Apps:	Is it allowed to use apps and mobile apps to deploy medical services and collect medical data? If yes, which type of individual/organisation can develop and employ these apps? Are there specific security requirements for these types of apps?
	There is no specific regulation to use mobile apps to deploy medical services or collecting data. *In the end the data protection law is applicable if any sensitive data is collected. If sensitive data is collected outside of switzerland the patient / person has to give his informed consent to every date (opt in) stored to the database.* *In practice most of the apps are not compliant.*
Institutions:	Do hospitals/clinics/labs employ apps to gather medical data? Is there a need for a medical treatment to permit the use of an app to process the medical data? Are there specific security requirements for the institutions collecting these data from the apps? Are medico-administrative data used by hospitals/clinics for management purposes?

	Yes they do. For professional apps the same rules as for other it equipment dealing with medical data are applicable (data protection law, cantonal medical law).
Tracking technologies:	Do hospitals/clinics/labs employ non-medical apps and devices to track and collect data from their patients? What type of data is collected? For what purpose? Is the data identifiable? Is the data combined with medical data?
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical apps and tracking apps? If yes, what are the standards?
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical diagnostic? How would this be applied to fitness and daily-basis data?
	For apps the same rules as for other it equipment dealing with medical data are applicable (data protection law, cantonal medical law) *If fitness and daily basis data is used for medical purpose same standards are applicable as for medical devices*

5. Medical Devices and Wearable Devices

5.1. Data Protection Issues:

A medical device can be defined as: 'any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application. Such a device should be intended by the manufacturer for one of a number of defined purposes, one of which is, diagnosis, prevention, monitoring, treatment or alleviation of disease' (Directive 93/42/EEC Article 1:2)

Some eHealth and mHealth devices and apps do not fall in this definition of medical devices, as can also be the case of a software working in combination with a physical device, for instance a smartphone.

5.2. Questions: Is your legal framework providing for a regulation of Medical Devices? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	For medical devices the remedies act is applicable
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
eHealth and mHealth:	Does the concept of Medical device in your country encompass services and apparels in the realm of eHealth and mHealth? What are the requirements? Should, for instance, the medical device be certified before it can be used?
	The remedies act covers all medical devices, software and all subjects which are intended to be used to influence positive a treatment.

	Medical devices must not harm patients, must work as promised the positive effect of treatment must be evident and provable.
Apps:	Does the concept of medical devices encompass apps? If yes, is there any regulation applicable to apps that perform medical services? Is there any regulation applicable on apps that track non-medical data that can lead to health information? If yes, what type of data?
	If the device is not intended for medical purpose, it is not a medical device whereas the remedies act is not applicable. If a seller intends to sell the device for medical purpose the remedies act is a applicable. *If non-medical data are used within a promise of a medical treatment and the app is sold for medical purpose the remedies act is applicable and the app will be treated as medical device.*
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical and/or wearable devices? If yes, what are the standards?
	If the device collects sensitive profiles of a person the data protection law or/and the telecommunication act are applicable.
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical treatment? How would this be applied to fitness and daily-basis data?
	It depends for what purpose the seller introduces the product. If the seller positions his product for medical purpose, it falls under the remedies act and will be treated as a medical device, independent of the collected data.

6. Internet of Things

6.1. Data Protection Issues:

Internet of things relates to common, ordinary devices that are now, and increasingly, connected to the Internet, such as cars, fridges, ovens, microwaves, etc. All of these devices can provide data that can lead to reveal information concerning one's health. A fridge can easily inform on the type of food stored and thus the diet of an individual. One of the biggest challenges of the Internet of Things is to guarantee the right to privacy and data protection in a world where every device collects, processes, analyses and transmits the data, commonly via wireless technologies.

In the realm of medical data, the issue mainly arises when crossing seemly unrelated data that can lead to health information about an individual.

6.2. Questions: Is your legal framework providing for a regulation of the Internet of Things? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	*The general data protection law is applicable if any data profiles are built up*
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).

Security:	What are the security standards that need to be employed by these devices when collecting personal data?
	Not directly specified. An appropriate security standard depending on the confidentiality of the collected data / profile must be achieved. Some minimal standards are defined.
Non-medical devices:	Are non-medical devices allowed to collect medical data, such as heart frequency? Are they allowed to cross medical data with non-medical data?
	Yes it is allowed as long as these devices are not intended to be for medical purpose. It is allowed to cross medical with non-medical data as long as no profile are built-up. If a behavior profile is built up or if collected medical data have an impact on privacy to this person or are linked to a person and a medical result may be interpreted these data become sensitive. On collecting sensitive data the general data protection law is applicable.
Privacy by Design:	Is there any requirement to implement privacy by design in the development of connected devices? If yes, what are the standards?
	It depends in the collected data, the concept privacy by design is not known in swiss regulation.

7. Electronic Doctor (online Doctor) and on-line appointments

7.1. Data Protection Issues:

The Doctor listens, talks and assesses the patient online, via a website, app, canal, sometimes including video-conference. Medical data is collected and processed, what are the security requirements and standards followed? Other websites provide for on-line appointments with doctors, which can also involve the processing of medical data.

7.2. Questions: Is your legal framework providing for a regulation of online Medical Treatment and is the on-line appointment system covered by such a framework? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	The telecommunication act is applicable. If any medical advice or result is produced by a software which is intended for medical purpose the remedies act is applicable as well.
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Medical treatment:	Is it allowed to perform medical treatment via online services? If yes, how should the medical services be provided? Does it have to follow the same requirements of a regular physically-present medical treatment?
	In general a medical treatment is allowed via online service but the health insurances are not allowed to pay for medical services within the regular insurance model.
Medical data:	How should the data collected via a medical treatment performed online be processed? Are there specific requirements? Which ones?

	There are no specific requirements, in general a medical doctor has to document the anamnesis, his decisions and treatments independent if he treats face to face or via online service.

Other comments and technologies
Should you wish to describe any technology, feature or trend that has not been covered by the questionnaire, please feel free to use the space provided below. Where relevant, also indicate recent legislation changes, guidelines and/or case law.

Urs Stromer, Walter Stüdeli, IG eHealth (info@ig-ehealth.ch)

URUGUAY

QUESTIONNAIRE

The questionnaire should ideally be completed by data protection authorities, health policy authorities, professional or patient associations as well as healthcare providers: you are invited to share it as widely as possible.

Please send your replies to dataprotection@coe.int no later than 15 December 2014.

1. Mobile Health (mHealth) and Electronic Health Records (EHR)

1.1. Data Protection Issues:

This is perhaps the biggest topic sitting at the intersection of technology and data protection. Mobile health (mHealth) and Electronic Health Records (EHR) are increasingly used in healthcare systems and provisions – it is a trend that needs to be examined.

Related to the EHR, these records are more accurate, cost-effective (in terms of storage) than paper-based notes. The concept of patient controlled/accessed EHR has been implemented in varying degrees in different countries.

Furthermore, some non-medical record can still contain health information about users and it should be considered if such records ought to be treated in a similar way to EHR.

Also, should 'medical data' as defined in Recommendation N° (97) 5 on the protection of medical data cover physical tracking data, such as pedometers or fitness data and data that can lead to medical information about an individual ?

1.2. Questions: if EHR exist in your country, is your legal framework providing for a regulation of such records? If mHealth exists in your country, is your legal framework providing for a specific regulation? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	EHR does exist in Uruguay. The legal framework is as follows: Laws Nº 18.331 of 11th August 2008 and Nº 18.335 of 15th August 2008. Presidential Decrees Nº 355/982 of 17th September 1982, Nº 396/003 of 30th september 2003, Nº 414/009 of 31st August 2009 and Nº 274/010 of 8th September 2010. There is no specific regulation on m-health. Law Nº 18.331 and Presidential Decree 414/009 provide the general framework for data protection.
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
EHR and Medical data:	What can be considered medical data in your country? Is it solely the data relating to a person's health (state, diagnosis, prognosis, medical treatment, etc.)? Is non-medical data that leads to medical information treated the same way as medical data (for instance in terms of confidentiality requirements)? Is the EHR solely constituted of data collected in a medical context or can the individual also himself or herself add information regarding his or her health?
	Health data is considered sensitive data (article 4 paragraph E of Law 18.331). Furthermore, article 4 paragraph D) of Decree 414/009 defines personal data related to health as "*any information regarding past, present and future physical and mental health of a person. Among others, data related to health may include the disability percentage or genetic information of a person*".

	Art. 18 of Law 18331 refers to treatment of sensitive data as follows: "*No person shall be forced to provide sensitive data. These can only be subject to processing with the express written consent of the data holder.* *Sensitive data can only be collected and subject to processing when involving reasons of general interest authorized by Act., or when the requesting body has the legal order to do so. These data can also be processed with statistical or scientific purposes when dissociated from the holders.* *The formation of databases which store information that directly or indirectly discloses sensitive data shall be prohibited. Except for those belonging to political parties, trade unions, churches, religious creeds, associations, foundations and other non-profit entities, the purpose of which is political, religious, philosophical, trade union, making reference to the racial or ethnic origin,* ***health and sex life,*** *regarding the data of their members or partners, even though the communication of said data shall always require the data holder's previous consent (...)".* *According to Art. 19 of Law 18331 "Public or private health institutions and professionals associated with health sciences may collect and process* ***personal data regarding the physical or mental health of patients that arrive there or that are or have been under their treatment,*** *observing the principles of professional secrecy, specific regulations and what is stated in this Act.".* As for possible sanctions in case of violations, art. 35 of the mentioned Law envisages as penalty measures:"*1) Warning. 2) Fine amounting to no more than five hundred thousand indexed units. 3) Suspension of the corresponding database".* Non medical data is not specially protected data, thought data protection principles and proceedures established in Law 18331 for personal data apply.
Sharing of data and Access:	Who is granted access to the EHR and how is the sharing of information (with other health care providers?) regulated? Where information is shared with pharmacists, is there a strict purpose limitation in place? How has the definition of the responsibility over the medical data been regulated?
	According to art. 30 of Presidential Decree Nº 274/010, access to the EHR is restricted to: a) the people responsible for the health care of the patient and administrative personnel regarding such care b) the patient or people authorized by the patient c) the legal representative of the patient that has been declared legally incapable d) the patient´s spouse, companion or closest relative, in specific cases e) the Ministry of Public Health Law 18831 art. 18 and Presidential Decree 396/003 art. 9 state that treatment of sensitive data can only be done with written and express consent of the holder. In addition, art. 15 of Decree 396/003 indicates that all data included in an EHR is the sole property of the person to whom it refers, and only he/she -or his descendants- can authorize it´s use by third parties. Art. 18 of Law 18.335 indicates that revealing the content of an EHR may be considered a felony under art. 302 of the Penal Code. General responsibility provisions are stated in the Civil Code.
Data quality:	Are the principles of legitimacy, fairness and minimisation applied to medical data? How are records kept accurate? How long is the data kept for, is the specific storage period defined for the EHR?
	According to Presidential Decree Nº 396/003 (Art. 8) and Law 18331 (art. 5) data protection principles apply to medical data. Art. 34 of Decree 274/010 establishes that the health-care providers must keep the EHR without any alterations and avoid destruction, according to the proceedures and requirements defined in other regulations. The HR may be destroyed following the proceedures established in Presidential Decree Nº 355/982 of 17th September 1982, but the destruction of EHR is not specifically regulated. This Decree distinguishes active HR from passive HR (the last ones being those HR that have not had any activity for a period of over 2 years and can be destroyed, with a previous and mandatory backup of the information).

	Art. 27 of Decree 274/010 indicates that all patients have the right to a complete HR, with information regarding the evolution of his/her health from birth until death. According to art. 29 of this Decree the correct completion of the HR is part of health-care, being responsibilty of the health-care personnel the complete, accurate, truthful, and comprehensible completion of the registration.
Data integrity:	Are any specific methods used to ensure the integrity of the data? How are patients identified in the EHR? In the context of research, are anonymisation methods used and what safeguards exist for re-identification?
	Article 20 of Law 18335 states that health-care institutions must ensure EHR content by any means necessary, although the Executive Power can determine uniform criteria for all EHR. According to the confidentiality principle established in art. 11 of Decree 396/003, the EHR must be structured in a way that enables the separation between the identification of the holder and the rest of the data. There are some mandatory standards established in the Decree, being one of them the identification of the patient by his/her National Identification Number. Article 12 of the above referred Law indicates that every medical research proceedure must be freely authorized by the subject of the research after receiving all the information in a clear way regarding the objectives and methodology, and only after the Bioethics Commision of the health-care institution has approved the proper protocol. The Bioethics Commision of the Ministry of Public Health must be informed in all cases. The information must include the right to revoke the given consent at any time.
Data security:	Where are the records stored? Is there a centralised database of EHR? What security technology is being used?
	There is not a centralized database of EHR. According to article 3 of Presidential Decree 92/014 of 10th April 2014 all of the Central Administration´s systems -referring to public institutions- must be located in safe Datacenters within Uruguay, with some exceptions. The Decree also provides some guidelines for the correct use of safe Datacenters in Annex III. Uruguay recently introduced the Oncological EHR, and is currently working in a national EHR as part of the objectives stated in the Technical and Interinstitutional Cooperation Agreement for the Development of the Salud.uy Program (http://www.agesic.gub.uy/innovaportal/v/4393/1/agesic/lanzamiento_de_la_historia_clinica_electronica_oncologica.html).
Rights of the person/patient concerned:	How can the right of access be exercised? How can the data be corrected? Can the person enter information in his or her own EHR? What are the legal remedies available?
	By means established in Law 18331 (Arts. 14 and 15) and Presidential Decree 414/009 (Arts. 9-13). According to article 14: "***Right of access.-*** *Any holder of personal data that previously proves his/her identity with the corresponding identity card or respective proxy, shall have the right to obtain any information on himself/herself registered in public or private databases. Said right of access shall only be exercised free of charge and at six-month intervals, unless a legitimate interest arises again according to the Legal Code"*. Article 15: "***Right to rectify, update, inclusion or deletion.-*** *Any natural or legal person shall have the right to request the rectification, updating, inclusion or deletion of their personal data included in a database, when verifying an error, falseness or exclusion in the information which the person is the holder of. The controller shall proceed to carry out the rectification, updating, inclusion or deletion, through the operations required for such purpose within a maximum term of five working days after receiving the request by the data holder or, otherwise, shall state the reasons why he/she/it considers it is not appropriate to do so. If the controller fails to comply with this obligation or upon the expiry of the deadline, the holder of the data shall be authorized to file the writ of habeas data provided for in this Act. The erasure or deletion of personal data shall not proceed, except in cases of:*

	A) Damages to the rights and legitimate interests of third parties.B) Obvious error or falseness. C) Contravention of a legal obligation. During the process of verification, rectification or inclusion of personal data, the controller, upon third parties' request to access reports on such data, shall record the fact that said information is subject to review. In the case of data transfer or communication, the controller must notify the rectification, inclusion or deletion to the recipient within five working days after the data processing is carried out. The rectification, updating, inclusion, erasure or deletion of personal data, when appropriate, shall be carried out free of charge for the holder". The DPA recently issued a Guide on Health Data Protection aiming at the general public with guidelines on how to exercise these rights (http://datospersonales.gub.uy/wps/wcm/connect/d4bcdc80440302c5b2c1f36d575befd1/guia-3-web.pdf?MOD=AJPERES&CONVERT_TO=url&CACHEID=d4bcdc80440302c5b2c1f36d575befd1)
Consent:	Is the system based on an opt-in approach? Is the principle of granular consent applied (with the possibility of preventing access to certain data?)? If yes, in which situations?
	As health data is considered sensitive data, previous, free, unequivocal, specific, and informed consent is required. Consent for personal data treatment must be distinguished from consent for medical treatment. Article 11 of Law 18.335 enables medical action without prior authorization in case of emergencies or grave risk of life.
Withdrawal:	Are patients able to withdraw the consent given to EHR schemes? If yes, what is the relevant procedure to withdraw such consent? What are the consequences?
	Yes. According to Law 18335 the person can withdraw the consent at any time (Art. 11). The withdrawal must be stated in the EHR.
Outsourcing processing of data:	Is outsourcing common? Under what circumstances? Where is the data outsourced to? What sort of safeguards are in place?
	Not Available.

2. Cloud Computing, Data Mining and Profiling from both Medical Records (including EHR) and Data not specifically related to medical records.

2.1. Data Protection Issues:

Cloud computing has brought a new dimension to the way data is stored, accessed and processed. Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS), Network as a service (NaaS) are all used by services and organisations that deal with both medical data and non-medical data.

With the development of more advanced and efficient data-mining and data-querying Medical techniques (e.g NoSQL, MapReduce, Hadoop) in conjunction with increased processing power and data storage, mining data has never been more informative, easier, and cost-effective.

Healthcare is a natural sector in which to apply new technologies and methodologies, with particular impacts in epidemiology, public health, health services research, etc.

Data that can lead to the identification of a particular individual and his/her health situation is not limited to medical data *per se,* present on Electronic Health Records, but also to unsuspicious type of information.

There is a growing concern that these schemes may be implemented in manner which does not always respect the patients' confidentiality and basic rights, and in a broader context, the use of this of information may prejudice the individuals concerned.

The ability to track and monitor patients and resources enables a more efficient provision of care but may have an impact on the right to privacy of the individual concerned.

2.2. Questions: Is your legal framework providing for a regulation of Cloud Computing, Data Mining and Profiling? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	Not specifically regulated. General DP Framework given by Law 18.331 of 15th August 2008 and Presidential Decree 414/009 of 31st august 2009.
Case-law:	
Other:	In a recent opinion issued by the Executive Council of the DPA (Nº 8/2014) the Authority determined that in the case of a backup service in which the databases are stored in international servers, there is an international transfer of data. It must be taken into consideration that both the service and the backup must be located on adecuate countries.

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Cloud computing:	How is cloud computing regulated in your country? Which security safeguards and standards are mandatory? Are there specific requirements in order to store medical data in the cloud? How is data shared and is the sharing regulated?
	Not regulated. General Data Protection Framework is applicable. We can mention article 3 of Decree 414/009: "*Territory. Personal data processing is applicable to the Act. that is being regulated when:* *A) They are performed by a database or processing controller established within the Uruguayan territory, and their activities therein carried out, whatever their legal type.* *B) The database or processing controller is not established within the Uruguayan territory, but uses media for data processing located within the country.* *All cases in which the above mentioned media are exclusively used for transfer purposes -as long as the database or processing controller appoints a representative with permanent domicile within the national territory before the Control Entity- so as to comply with the duties included in the Act. that is being regulated and in this regulation are exempt from the foregoing rule. Such appointment shall not prevent any legal actions that might be filed against the database or processing controller and shall not reduce his/her responsibility regarding the compliance of legally or regulatory imposed duties*". Article 4 H of the above mentioned Decree is also applicable: "*Article 4. Definitions. For the purposes of this regulation, and without prejudice of the definitions contained in the Act. That is being regulated, the following definitions are considered: H) International transfer of data: data processing that implies their transmission outside the national territory, thus becoming an assignment or communication by the database or processing controller established within the Uruguayan territory*".
Government:	Do governmental programmes exist to allow for increased data-mining of medical records? If yes, what are the purposes of this data mining? Are private entities allowed to access the data? Under what circumstances? What sort of techniques and technologies are being used? To what end? Are data subjects informed of this type of data-mining?
	Not Available.
Private sector:	Are private entities allowed to mine medical data which they process? Under what circumstances? Can the government have access to this data?

	Not Available.
Profiling:	Are the government and the private sector allowed to employ profiling methods on medical data? If yes, under what circumstances? Is it allowed to cross and correlate non-medical data with medical data?
	Not Available.

3. RFID and wireless communication technologies

3.1. Data Protection Issues:

It is common for medical devices, such as patients' tags, to possess RFID technologies in order to facilitate the transmission of the patients' data.

It can also be related to the data-mining operations previously mentioned as it is another category of information that can be used to discern meaningful patterns.

Transmission of data through radio-frequency is not limited to medical devices. Almost any smartphone uses some technology enabling to collect, and share, the user's data. For instance, via WI-FI it is possible to identify users' locations and therefore infer some of their behaviour, which in some cases can relate to health information.

3.2. Questions: Is your legal framework providing for a regulation of RFID technologies and the transfer of personal data through wireless technologies? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	Not specifically regulated. General DP Framework given by Law 18331 of 15th August 2008 and Presidential Decree 414/009 of 31st august 2009.
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
RFID:	How is RFID used in hospital/clinics for (a) resource management, (b) patient care? What types of database systems (and security) are implemented in conjunction with RFID use? How are issues of access, sharing, consent etc. managed considering that RFID may be used without the patients' knowledge.
	Not Available.
Wireless tracking technologies:	Are hospitals/clinics employing other wireless tracking technologies besides RFID? Which ones? Do they have to follow specific security requirements? Which ones?
	Not Available.

4. Applications (Mobile)

4.1. Data Protection Issues:

Information society is increasingly relying on the use of "apps" (application), most of them mobile. These apps are commonly designed to gather personal data, and in practice often process medical data.
Technologies such as multi-touch touchscreen, accelerometers or gyroscopes, ambient light sensors, GPS and cameras, and devices featuring fingerprint and biometric sensors also involve the collection of medical data.

A mobile phone application can monitor accurately physiological data, such as heartbeats, sleep patterns, fitness information.

4.2. Questions: Is your legal framework providing for a regulation of Apps and Mobile Apps? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	Not specifically regulated. General DP Framework given by Law 18331 of 15th August 2008 and Presidential Decree 414/009 of 31st august 2009.
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Apps:	Is it allowed to use apps and mobile apps to deploy medical services and collect medical data? If yes, which type of individual/organisation can develop and employ these apps? Are there specific security requirements for these types of apps?
	Not Available.
Institutions:	Do hospitals/clinics/labs employ apps to gather medical data? Is there a need for a medical treatment to permit the use of an app to process the medical data? Are there specific security requirements for the institutions collecting these data from the apps? Are medico-administrative data used by hospitals/clinics for management purposes?
	Not Available.
Tracking technologies:	Do hospitals/clinics/labs employ non-medical apps and devices to track and collect data from their patients? What type of data is collected? For what purpose? Is the data identifiable? Is the data combined with medical data?
	Not Available.
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical apps and tracking apps? If yes, what are the standards?
	Not Available.
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical diagnostic? How would this be applied to fitness and daily-basis data?
	Not Available.

5. Medical Devices and Wearable Devices

5.1. Data Protection Issues:

A medical device can be defined as: 'any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application. Such a device should be intended by the manufacturer for one of a number of defined purposes, one of which is, diagnosis, prevention, monitoring, treatment or alleviation of disease' (Directive 93/42/EEC Article 1:2)

Some eHealth and mHealth devices and apps do not fall in this definition of medical devices, as can also be the case of a software working in combination with a physical device, for instance a smartphone.

5.2. Questions: Is your legal framework providing for a regulation of Medical Devices? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.	
Legislation:	Not specifically regulated. General DP Framework given by Law 18331 of 15th August 2008 and Presidential Decree 414/009 of 31st august 2009.
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
eHealth and mHealth:	Does the concept of Medical device in your country encompass services and apparels in the realm of eHealth and mHealth? What are the requirements? Should, for instance, the medical device be certified before it can be used?
	Not Available.
Apps:	Does the concept of medical devices encompass apps? If yes, is there any regulation applicable to apps that perform medical services? Is there any regulation applicable on apps that track non-medical data that can lead to health information? If yes, what type of data?
	Not Available.
Privacy by Design:	Is there any requirement to implement privacy by design in the development of medical and/or wearable devices? If yes, what are the standards?
	Not Available.
Consent:	Is the system based on an opt-in approach? Is it necessary for the collection to be in reference to a medical treatment? How would this be applied to fitness and daily-basis data?
	Not Available.

6. Internet of Things

6.1. Data Protection Issues:

Internet of things relates to common, ordinary devices that are now, and increasingly, connected to the Internet, such as cars, fridges, ovens, microwaves, etc. All of these devices can provide data that can lead to reveal information concerning one's health. A fridge can easily inform on the type of food stored and thus the diet of an individual. One of the biggest challenges of the Internet of Things is to guarantee the right to privacy and data protection in a world where every device collects, processes, analyses and transmits the data, commonly via wireless technologies.

In the realm of medical data, the issue mainly arises when crossing seemly unrelated data that can lead to health information about an individual.

6.2. Questions: Is your legal framework providing for a regulation of the Internet of Things? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	Not specifically regulated. General DP Framework given by Law 18331 of 15th August 2008 and Presidential Decree 414/009 of 31st august 2009.
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Security:	What are the security standards that need to be employed by these devices when collecting personal data?
	Not Available.
Non-medical devices:	Are non-medical devices allowed to collect medical data, such as heart frequency? Are they allowed to cross medical data with non-medical data?
	Not Available.
Privacy by Design:	Is there any requirement to implement privacy by design in the development of connected devices? If yes, what are the standards?
	Not Available.

7. Electronic Doctor (online Doctor) and on-line appointments

7.1. Data Protection Issues:

The Doctor listens, talks and assesses the patient online, via a website, app, canal, sometimes including video-conference. Medical data is collected and processed, what are the security requirements and standards followed? Other websites provide for on-line appointments with doctors, which can also involve the processing of medical data.

7.2. Questions: Is your legal framework providing for a regulation of online Medical Treatment and is the on-line appointment system covered by such a framework? If not, how is the general data protection legislation applied to cover it? Please indicate the legislation (as well as possible sanctions envisaged in case of violations), guidelines, DPAs' opinions and/or case law.

Legislation:	Not specifically regulated. General DP Framework given by Law 18331 of 15th August 2008 and Presidential Decree 414/009 of 31st august 2009.
Case-law:	
Other:	

Specific questions (for each section, please indicate where possible recent legislation changes, guidelines, DPAs' opinions and/or case law).	
Medical treatment:	Is it allowed to perform medical treatment via online services? If yes, how should the medical services be provided? Does it have to follow the same requirements of a regular physically-present medical treatment?
	Not Available.
Medical data:	How should the data collected via a medical treatment performed online be processed? Are there specific requirements? Which ones?
	Not Available.

Other comments and technologies
Should you wish to describe any technology, feature or trend that has not been covered by the questionnaire, please feel free to use the space provided below. Where relevant, also indicate recent legislation changes, guidelines and/or case law.