COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 15 June 2015 T-PD(2015)07

INTRODUCTORY REPORT FOR UPDATING RECOMMENDATION R (97) 5 OF THE COUNCIL OF EUROPE ON THE PROTECTION OF MEDICAL DATA

By Jeanne Bossi Malafosse
DLA Piper France LLP legal consultancy

Directorate General of Human Rights and Rule of Law

Summary of contents

I- Introduction: context of health data protection in 2015

The development of digital technology over the last few years has led to an outright “datification” of our societies. Data are everywhere. World activity will produce more data during the next two years than it produced since the beginnings of information technology. These data constitute a valuable raw material and a world growth factor expected to represent, for Europe, no less than 8% of European GDP by 2020.

The health sector is no exception to these trends. The new environment is typified by growing computerisation of the professional sector and especially activities relating to care and prevention, life sciences research, health system management, and moreover the growing involvement of patients.

Mobility phenomena, as well as the development of connected medical objects and apparatus, now contribute to the exponential growth in the volume of data produced; the “Big data” phenomenon simply reflects the peculiarities of processing large masses of data with their demands as to processing speed, disparity of data and creation of special value.

Health data thus represent unique interests and a potential for creating value and furthering public health, the attainment of which will depend on the ability of states to organise the development of an ecosystem facilitating their use while guaranteeing respect for privacy and confidentiality of personal data.

States in fact face major challenges today, for which health data processing can and already does perform an essential role: these relate to public health notably with the spread of chronic diseases, to the quality of care, medical transparency and democracy, efficiency of the health system in a context of growing health expenditure and chronic deficit in the welfare accounts, as well as to innovation and growth in such varied and important fields as personal medicine and information technologies.

E-health, that is use of information and communication technologies in the health sector, emerges as a powerful impetus for quality, safety and efficiency of care, clearly identified by the authorities. Information systems and digital technologies generally will be one of the principal vehicles for improving the quality, organisation and efficiency of health systems through the present decade.

These multiple challenges present themselves in very different terms today than in 1997, the date of Council of Europe Recommendation R (97) 5 on the protection of medical data.

Indeed, the development of the new information and communication technologies in the fields of health and medical welfare, compounded by the above-mentioned challenges which societies face, has had a systemic effect on the organisations and on the role of the various care providers.

The need for exchange and sharing of health data in the interests of better provision for individuals has become crucial and considerably alters the very nature of the relationship between carers and those cared for, which a few years ago was still founded on a sacrosanct personal exchange. The patient today is active and, even while not realising the full implications of it, wishes to control his treatment, his data and how they are processed.

Of course, personal health data allowing an individual’s identification are always liable to lay bare the intimacy of private life and on that account the law should continue to confer a special status on them and to impose compliance with rules aimed at guaranteeing their confidentiality.
Preservation of professional (medical) secrecy is and should remain central to this guarantee.

The future Council of Europe Recommendation intended to update or supersede the 1997 one will need to take account of these trends: how to facilitate the development of the virtualised health data exchange needed to improve the arrangements for treatment and care of persons without, however, renouncing the fundamental principles of protection of privacy?

This new Recommendation is also to take into account the principles of the present draft General Data Protection Regulation which already accommodates the major developments which have occurred since Directive 95/46 of 24 October 1995, particularly the principle of *Privacy by design* which requires data protection to be incorporated from the inception of the systems potentially processing the data.

The purpose of the following considerations is to propose new directions for recasting the text of the 1997 Recommendation. They are firmly placed in a perspective where digital technology is no longer a question but a reality. They are fuelled by the analysis which has been made of the questionnaires sent to the Council of Europe member states, a presentation of which is appended, and by the analysis which can be made today of how digital technology is used in the health sector.

II- Directions for a new recommendation

1. A new scope to be defined

The definitions introducing the Appendix to Recommendation No. R (97) 5 are to be reviewed and amplified. While the definition of personal data is retained, it is supplemented by other definitions whose purpose will be to clarify the terms used in the recommendation and which thus reflect the new scope of the text.

1.1 Personal health data

In the first place, the expression "*health data*" will henceforth be preferred to "*medical data*".

In concrete terms, these are data capable of disclosing a person's state of health. This indication would also be consistent with the definition of health data arising from the Proposal for a Regulation of the European Parliament and the Council of 5 January 2012 on data protection: *all data pertaining to the physical or mental health status of a data subject or to the provision of health services to that person*. It conveys a broader concept of health data which today cannot be limited to the sole indication of a complaint, so much does a person's health provision also entail knowledge of his/her family or social situation and involve multiple operators, professionals in the health and welfare sectors.

Personal health data thus covers, in particular, all information relating to the identification of the patient in the care system or the device used for gathering and processing health data, all information obtained during a medical check or examination including biological samples and genome data, all medical information such as an illness, a disability, a risk of illness, a medical record, a clinical treatment or the physiological or biomedical condition of the person concerned, irrespective of its source, whether originating for example from a doctor or other health professional, a hospital, a medical facility or in vitro diagnostic testing.

Medical welfare data refer to all data generated by professionals practising in the general welfare and medical welfare sector, participating in the medical care of the person concerned by, for example, helping to characterise his/her state of health. For the sake of simplification, the term personal health data also covers the term medical welfare data.

Besides, the Article 29 Working Party published on 5 February 2015, at the request of the European Commission, an opinion on criteria to be considered for defining health data, particularly when they relate to lifestyle and to wellness applications[1].

[1] Three categories were thus distinguished: a) Data processed by the application or apparatus are intrinsically / plainly medical data. In other words, the data provide information on an individual's state of physical or mental health which is generated in a professional context of health (for example, health care providers); b) raw data from the sensor processed by the application or apparatus may be used separately or in conjunction with other data to draw conclusions on an individual's state of health or real health hazards; c) data allowing conclusions to be drawn as regards an individual's state of health (irrespective of their accuracy or inaccuracy, lawfulness or unlawfulness, adequacy or inadequacy).

In the second place the concepts of *"anonymisation"* and *"pseudonymisation"* also need to be defined, so widespread today are the techniques to which they refer, particularly as regards re-use of health data for research purpose or in the context of Big data for instance. Anonymisation is the outcome of processing personal data so as to prevent, irreversibly, all identification. It constitutes a further stage of personal data processing. Pseudonymisation, not a method of anonymisation, simply lessens the correlation of a data set with the original identity of a subject. It is a useful security measure.
Pseudonymised data continue to permit profiling of a subject and correlation between different data sets.[2]

Proposal No. 1

- Define health data broadly to include all information that might characterise an individual's state of health, deliveries of health services provided, and the person's medical welfare environment.

- Define the concepts of "anonymisation" "pseudonymisation".

1.2 Exchanging and sharing personal health data, and information systems

It is plainly necessary to define the concepts of exchanging and sharing personal health data in that these concepts now reflect the reality of medical practice and enable the different players, professionals and patients alike, to manage health data, for which information systems form tools that allow the development of exchange and sharing.

While respect for privacy and medical secrecy are two fundamental rights of the patient, medical secrecy binds all health professionals. But in order to ensure continuity of care or to determine the best possible provision, health professionals now need to exchange information on the patients of whom they take charge. This "shared secrecy" concept is generally recognised by law which also defines its limits. However, the patient must still be able at all times to refuse the disclosure of information concerning him or her to one or more health professionals.

Data exchange might be defined as the communication of information to a clearly identified recipient or recipients by a known transmitter. Use of a secured e-mailing facility is one example.

Conversely, the principle of data "sharing" means making information accessible to third parties not necessarily identified at the time of the pooling, and according to a principle of permissions. Sharing thus carries particular risks due to the retention of the data, but thereby allows information serving co-ordination and continuity of care, or the person's interest, to be made available to several professionals entitled to be acquainted with it. The principle of a shared electronic medical record is an example.

Sharing and exchange of personal health data are commanded firstly by the development of interoperable data processing systems and secondly by the use of common reference frameworks among professionals.

Health information systems, which today constitute the virtualised medium for circulation of health data, must also be covered by the definitions. Indeed, the digitisation phenomenon observed in the health sector as in others has altered the rules of urbanisation of information systems which must henceforth be characterised by their interoperability. Interoperability is surety for the expression of the rights of persons. Storage of personal health data in proprietary formats denying access may constitute a restriction on the exercise of rights.

[2] Cf. Opinion 05/2014 on anonymisation techniques adopted on 10 April 2014 by the Article 29 Working Party on data protection.

Proposal No. 2

- Define the concepts of exchanging and sharing health data.

- Define the terms “urbanisation of health information systems” and “interoperability”.

1.3 Hosting of health data and *Cloud computing*

Outsourcing to third entities in order to have health data kept on the Internet in a secure and lasting manner has today become an effective means to manage databases and ensure storage at low cost. The term *Cloud Computing* is used to designate the various Internet storage modes for these bases: Saas (*Software as a service*), Iaas (*Infrastructure as a service*) and Paas (*Platform as a service*).

This term should be defined in the recommendation, for the processing of health data does not develop today without these new infrastructures.

Recognition of the role played by services platforms and of their responsibility in processing the data which they host illustrates this, and will need to be dealt with in the future recommendation.

1.4 Mobile health (connected medical devices and objects)

The mobile health developing for some years in all countries (as the answers to the questionnaire show) materially corresponds to the use of objects connected in an Internet of Things for purposes of health data management. This development takes various forms and comprises several categories of applications, themselves pursuing very different ends in their use. From the medical device regulated today at European level to the “*mHealth*” or “*quantified self*” applications, it is plainly necessary to lay down certain principles of health data use and of processing by such connected objects, one of whose major characteristics is to boost the quantity of data produced.

Traditionally in fact, the item of care produces the data item - a visit to a health professional generates a medical record. These tools will in future produce data having an impact on the care itself.

In particular, trying to mark the boundary of “wellness” applications not subject to the same requirements as those clearly pursuing an aim of health care seems useful for better defining the players’ obligations (Cf. footnote 1 on the various categories identified by the Article 29 Working Party).

Proposal No. 3

- Define the terms hosting/Cloud Computing.

- Define the term “mobile health”, distinguishing the wellness from the health care purposes and the data produced by the patient personally and on his/her responsibility from those produced with the intervention of professionals (health and medical welfare sector).

2. Legal framework of personal health data processing

2.1 Principles of personal data protection

It should be recalled that personal health data can only be processed in the cases determined by domestic law, and at all events in a manner respecting professional secrecy, the privacy of individuals and the confidentiality of their information.

The principles governing personal data protection as set out in the Council of Europe Convention of 28 January 1981 and made explicit in Directive 95/46 of 24 October 1995 must also be observed.

They should be recalled in the body of the draft Recommendation as a general, mandatory framework: a specific and legitimate aim of processing, relevant data, limited data storage time,

introduction of security measures such as to guarantee the confidentiality of the data, and respect for the right of individuals and their information.

Today however, in view of a context which has changed radically, these five golden rules of data protection should allow of adaptation to the de-partitioning of exchanges between professionals and patients and to the care pathway concept which today characterises provision more than the traditional special relationship between a professional and a patient, even if this endures.

While it still appears necessary to list the different purposes for which health data may be collected and processed, regard should also be had to the fact that the development of connectivity of objects, for example, vastly increases the number of data items produced, moreover for purposes not always easy to foretell.

Nowadays, traditional data protection principles are not always readily applicable to this "datification" phenomenon, Big Data being a practical example of it. [3]

It is thus plainly important to specify, alongside the conventional purposes of medical data processing, the ability of states to provide for a non-predetermined use as long as it complies with the principles of confidentiality and privacy of individuals and is under the control of the national data protection authority.

By way of an illustration, authorisation should be given to the possibility afforded today by Big Data for identifying public health problems not determined beforehand but henceforth made knowable by the analysis of a larger quantity of data.

Likewise, the concept of data controller should today take into account the absence of material boundaries to data transfers and the undeniable new responsibility of Internet platforms in carrying out processing, as well as the fact that the purposes and procedures of one processing operation are now often determined by multiple individuals.

At all events, it still rests with the national data protection authorities to satisfy themselves that these principles are observed and to disseminate all recommendations calculated to ensure compliance with the "*Privacy by design*" principle.

2.2 Recognition of shared professional secrecy

The present health policies pursued in Europe especially stress the need for co-ordination of the operators acting at every stage of the patient's treatment pathway, in particular with the help of information systems. This pathway has a configuration not restricted to care and revolving round preventive, health, medical welfare and general welfare aspects. It has ramifications in time (arranging co-ordinated, organised provision for the patient) as well as in space (arranging the provision within an area, in the vicinity of the home).

This de-partitioning between the players in the health and medical welfare sectors materialises in the creation of new facilities for collaborative practice and of new practice patterns which must be able to rely on legal recognition of shared secrecy.

The development of electronic medical records and of collaborative platforms requires this advance, the principle of which is already established in many countries. France for example is preparing to pass a statute substantially widening the concept of healthcare team to permit sharing and exchange by professionals in the health, medical welfare and general welfare sectors without infringing professional secrecy and involving their responsibility. Of course this shared secrecy must be limited to the patients cared for in common and not raise objections from them.

[3] "Big Data" refers to sets of data which become so voluminous as to become difficult to process with only database management tools or conventional information management tools.

Big Data also denotes the whole of the technologies, infrastructures and services for collecting, storing and analysing data gathered or produced in growing quantity, thanks to automated processing and to reliance on technologies of artificial intelligence (Report by the Institut Montaigne, " Big data et objets connectés", 2015).

Proposal No. 4

- Recall the major principles of personal health data protection while incorporating, via the "*privacy by design*" principle, the concept of conformity with a framework which permits adjustment as regards the purposes of data gathering and processing and as regards designation of the data controller(s).

- Recognise professional secrecy shared between health professionals caring for the same patients.

3. A secured functional framework suited to the new urbanisation of health information systems

3.1 Interoperability reference architecture

Medical data processing today avails itself of new process architectures for management (Saas for example) or storage (Cloud). This new computing environment must permit communication in accordance with legally defined principles.

Certain reference frameworks for technical, security and organisational uses should accordingly be defined by the authorities of each state to assure the citizens that their health data are well-managed with proper respect for their confidentiality and privacy.

These reference frameworks need a legal basis to be authoritative and allow the technical and semantic interoperability of information systems, without which there can be no effective exchange and/or sharing.

They are founded on international norms and standards allowing present and future computer products or systems to communicate, hence use a common language (semantic interoperability) and common technical reference frameworks (technical interoperability).

The specifications and tools of the interoperability framework for health information systems are modular and divided into three strata: a stratum of interoperable contents, concentrating the means of semantic interoperability – that is the structuring and the meaning of the information exchanged between the health information systems, a stratum of interoperability services and a transport stratum, which together represent the reference framework's core of technical interoperability. [4]

Without going into such detail, the future recommendation on health data processing should make reference to the above.

Proposal No. 5

- Make the principle of conformity to interoperability reference frameworks enforceable.

- Leave the organisation of their updating to the states.

[4] The most widespread international standards are the IHE standards "*Integrating the Healthcare Enterprise*"/HL7 "*Health Level Seven*" which correspond respectively to the production of existing standards profiles compatible with given uses and to the development of interoperability standards in the health field. On the basis of these reference frameworks, electronic medical document formats (CDA, *Clinical Document Architecture)* are defined.

3.2 Security reference frameworks

The confidentiality of personal health data is consubstantial with the principle of professional (medical) secrecy and constitutes one of the essential principles of personal data protection.

The data processing security allowing compliance with this confidentiality to be assured today represents an even more compelling concern in that the multiplication of exchanges gives a greater number of persons access to the data. Policies on permissions and traceability are essential for ensuring the protection of data and preventing their disclosure to unauthorised third parties.

The virtualisation of exchanges in the health sector has brought about a modification of the type of measures taken to achieve this security.

Besides the still important conventional measures of physical and logical security, the security policy which it behoves the data controller to establish is also underpinned today by security reference frameworks whose proper application the public authorities need to ensure.

These reference frameworks are in general organised according to their type and the target of their application.

They are:

- organisational reference frameworks defining the organisation of security and setting out the good practices directed at health professionals;
- technical reference frameworks describing the methods for authenticating patients, health operators and accountability of documents, for example where intended more for industrial users;
- specific reference frameworks intended for data controllers in connection with specific applications like Internet of Things or maintenance rules;
- legal reference frameworks aimed at providing information on the regulation of special circumstances of practice.

The legal foundation given to these reference frameworks should be sufficiently high up in the hierarchy of norms to be binding, but the specifics of the technical measures should be adaptable to developments in data processing techniques and to the state of the art.

- Thus the reference frameworks for identification of players appear indispensable for health professionals' quality assurance. Prioritise the use of professional directories regularly reviewed using from data certified by an authority whose task this is.

The same should apply to the patient where the data recorded and used enter into a care relationship, and it is therefore imperative for health data not to be assigned to the wrong patient. The need for reliable, lasting identification is a security guarantee, of importance for tracking the patient throughout his sequence of care.

- Development of the activity of hosting personal health data bases also necessitates making sure of the conditions under which the data are stored and released to the users. Particular hazards linked chiefly with the location of the data, loss of control of the information system and mutualisation of resources must therefore be identified.

It is a matter of organising the deposit and storage of health data under such conditions as to guarantee their continuity and confidentiality, and of making them available to authorised persons.

It rests with states to satisfy themselves that these principles are observed and to apply the necessary guarantees.

Proposal No. 6

- Recall the importance of security measures in the handling of health information.

- Make the reference frameworks identifying the players, both professionals and patients, enforceable.

- Organise the activity of health data hosting.

4. Rights of the individual

4.1 A right to information enhanced by *empowerment*

Respect for the rights of individuals is central to personal data protection. The right to information at the time of the gathering, recording or communication of the data, the right of direct access to health data and the right of rectification must be secured by all states to their citizens.

Whatever the situation in which the health professional practices, the patient must be informed as to his/her state of health and the nature of the care administered. This rule illustrates the traditional principles of information and trust that characterise the unique relationship of the doctor, and more generally of any health professional bound to observe secrecy, with the patient.

The content of the information must concern the purpose of the treatment (administration of care, research, etc.), the compulsory or optional nature of replies and the consequences of failure to reply, and the identity of the data controller and the data recipients. In addition, the patient must be informed as to the existence of his rights and the manner of their exercise and, where relevant, of data transfers to countries outside the European Union.

Everyone must also retain the possibility of objecting, for legitimate reasons, to the processing of their health data. Exceptions may be prescribed by legislation operating within the member states to the extent justified by another legitimate interest.
As regards information prior to care, it will be emphasised that the person must also receive information on the kinds of technology employed (telemedecine, cloud hosting, etc.).

Each health professional informs patients, within the limits of his/her competence and in a suitable, useful and relevant way having regard to their state of health and ability to understand.

The cases where the health professional may waive this duty of prior information are restrictively enumerated and left to the professional's own discretion: cases of urgency, cases where it is impossible to inform the person.
A person's wish to be kept in ignorance of a diagnosis or prognosis should be complied with, except where third parties run a risk of transmission.

The draft European regulation on data protection in the process of adoption, by reinforcing the right to deletion and portability of data, irrespective of who controls processing, establishes the concept of *empowerment*, that is the subject's control over his/her data at all stages of its life cycle; however, this concept has particular implications in the health sector.

Indeed, the development of connectivity of objects enabling patients to be more active in their medical care lends a new dimension to the right to information as it is presented.

The data controller is no longer alone in holding information and in conveying its content to the patient. Recognition of the right of direct access to medical data, and the technical command which some patients have over their data by means of digital tools, makes the relationship more balanced.

4.2 Obtaining consent

The point to be dealt with here is consent to processing of health data, not consent to treatment which, subject to some exceptions, remains an incontrovertible constraint.

Consent must be purely the expression of agreement to the use, sharing and exchange of health data under assured conditions of security and with clear prior information.

The stipulation of consent should not shield or exonerate the person responsible for obtaining it from compliance with security measures or from the effort to inform, which is the actual protection for individuals today.

Efforts ought not to focus disproportionately on the act of obtaining this consent in whatever form, but on what it embodies by way of requirements. If consent is a legal safeguard, it is not necessarily an ethical guarantee.

Thus there arise the questions of its form, how obtained and the cases where it must be obtained. Where it is stipulated, it must be clear and unequivocal, explicit and prior to and/or concomitant with the collection and recording of the information.

It must remain reversible and controlled by the patient and, since its expression may be virtualised today, traceability of the accessing of health data constitutes the technical means of ensuring respect for the patient's rights and is an essential guarantee.

Exceptions to the obligation to obtain consent, when it is stipulated, should be provided for and are a matter of the health professional's discretion. Urgency or impossibility of obtaining the patient's consent in view of his/her condition may form exceptions which can be managed by the patient's naming a trusted individual who will decide in his/her place.

Proposal No. 7

- Strengthen patients' rights over their health data by incorporating the concept of empowerment.

- Limit the recording of consent to cases where domestic law expressly provides for it.

5. Re-use of health data

Personal health data collected for a given legitimate purpose can be re-used for other purposes in certain cases. In general, the domestic law of countries prescribes specific guarantees.

Purposes of research in the health field in all its forms: epidemiological, biomedical, statistical, historical, etc. are to be covered.

These possible re-uses are essential to public health since the results of such research are the basis on which states are able to identify particular health problems and take the necessary steps for remedying them and/or for framing their health policy.

The so-called secondary purpose of health data is improvement of public health.

This is traditionally pursued on the basis of research in the health field whose procedures are specified by national legislation and subject to the principles of personal data protection.

But today, with the potential of Big data and the proliferation of data generated by the use of connected objects, whatever they may be, it is observed that the classical criteria of re-use founded on the principles of personal data protection need to be assessed against this new environment.

Health data are produced by very varied sources, and it is important for researchers and observers to be able to collate them with other sources of data (environmental, climatic, social, for example).

The debates on opening up databases in conjunction with the new potential offered by Big data should lead to the creation of a favourable legal environment for secondary use of health data beneficial to prevention of risks and improvement of public health.

In that connection, while the principles of protecting personal health data should be reaffirmed, they are not to be applied and/or interpreted as impeding secondary use of health data except where no advantage is to be gained from the knowledge which analysis of the data masses produced today can bring economic players as well as public authorities.

Here, anonymisation techniques as defined earlier are not sufficient, so instructive is the profiling of behaviour patterns.

The pseudonymisation techniques allowing this profiling and the correlation of data sets should be encouraged, assessed in the light of the real risks of re-identification, and not subjected to undue constraints by the member states.

Proposal No. 8

- Adapt to the new context of proliferation of health data the regulatory framework allowing secondary use of such data for purposes of improving public health.

III- Appendices

1. Analysis of the replies to the questionnaire sent to member states

Summary of Compilation of Replies on Medical Technologies and Data Protection Issues:
Recommendation No. (97) 5 on the protection of medical data

The Consultation Committee of the Convention for the protection of individuals with regard to automatic processing of personal data issued a Questionnaire on Medical Data to the member States of the Council of Europe. The compilation of replies that has been sent to us for review is not exhaustive since it comprises a total of 36 replies some of which are incomplete (re identified by the following caption). Furthermore, only 20 States out of 47 have answered the Questionnaire, namely: Albania, Austria, Belgium, Bosnia, Croatia, Estonia, Latvia, Lithuania, Germany, Hungary, Italy, Monaco, Norway, Poland, Portugal, Serbia, Slovakia, Macedonia, Switzerland and Uruguay. This being said, we can only assume that the following restitution is as accurate as possible and will formulate in a separate paper recommendations on that basis.

1. Mobile Health and Electronic Health Record

- Does EHR exist in your country?

	AL	AU	BE	BO	CR	ES	LA	LIT	HU	GE	IT	MO	NO	PO	PO	SE	SL	MA	SW	UR
No EHR									√			√	√					√		

Under Construction		√		√				√						√		√				
EHR	√		√		√	√	√			√	√				√		√		√	√

Few States have specific definition enshrined in dedicated health or e-health regulation. When such regulation does not exist, States rely on general data protection law. When applicable, EHR is restricted to health data.

- Are there specific mHealth regulations in your country?

There does not seem to be any m-Health regulation enacted to date in the concerned States.

- Who is granted access to EHR?

	AL	AU	BE	BO	CR	ES	LA	LIT	HU	GE	IT	MO	NO	PO	PO	SE	SL	MA	SW	UR
Authorized medical staff	√	√	√	√	√	√	√		√	√	√	√	√	√	√	√	√	√	√	√
Competent Authorities			√		√	√	√	√			√			√				√		√
Pharmacists (stricter access)		√	√				√			√	√			√						

More generally, the Data Controller is responsible for purpose limitation and for information security. Some States provide different levels of authorization. For instance, Croatia has 4 levels of authorizations (no access, limited access, full access, special access).

- Do you use anonymisation technique?

	AL	AU	BE	BO	CR	ES	LA	LIT	GE	HU	IT	MO	NO	PO	PO	SE	SL	MA	SW	UR
Yes		√	√			√	√	√		√	√	√			√					
No	√				√								√							

- How are patients identified in the EHR?

	AL	AU	BE	BO	CR	ES	LA	LIT	GE	HU	IT	MO	NO	PO	PO	SE	SL	MA	SW	UR
By name and surname	√									√	√									
Identification Number		√	√			√	√	√		√	√		√		√			√		√

- How long is the data kept?

Concerning data retention, there is often no specific storage period defined for EHR. However conservation time varies depending of the type of records and methods. For instance in Albania, health records are stored 30 years, discard reports 50 years, imaging diagnostic methods 10 years, recipes pharmacies 2 years except for narcotic and psychotropic 5 years.

- Where are the records stored?

	AL	AU	BE	BO	CR	ES	LA	LIT	GE	HU	IT	MO	NO	PO	PO	SE	SL	MA	SW	UR

Centralized system	√					√	√					√		√	√	√	√			
Decentralized system		√	√	√					√		√	√								√

- Is the system based on an opt-in approach?

	AL	AU	BE	BO	CR	ES	LA	LIT	GE	HU	IT	MO	NO	PO	PO	SE	SL	MA	SW	UR
Opt-in	√		√						√		√						√		√	
Opt-out		√		√	√	√	√	√		√		√	√		√	√				√

- Are patients able to withdraw their consent?

In every State, withdrawal of consent is possible at any given moment.

	AL	AU	BE	BO	CR	ES	LA	LIT	GE	HU	IT	MO	NO	PO	PO	SE	SL	MA	SW	UR
Yes	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√

- Is outsourcing common?

	AL	AU	BE	BO	CR	ES	LA	LIT	GE	HU	IT	MO	NO	PO	PO	SE	SL	MA	SW	UR
Yes		√				√		√				√		√		√	√		√	
No	√		√		√		√			√	√									

For instance, Austria uses outsourcing within the autonomy and responsibility of the health service providers as long as the storage is based in the EU. Lithuania enables outsourcing only if it is executed on legal basis of agreements.

2. Cloud computing, Data mining and Profiling

- Is your legal framework providing for a regulation of Cloud Computing?

	AL	AU	BE	BO	CR	ES	LA	LIT	GE	HU	IT	MO	NO	PO	PO	SE	SL	MA	SW	UR
Specific provisions		√																		

Cloud computing is not specifically regulated, except in Austria where legislation stipulates that health data which are saved by means of cloud computing have to be encrypted state-of-the-art. Most often, cloud computing is regulated by non-binding guidelines issued by National Data Protection Authority.

- Is your legal framework providing for a regulation of Data Mining?

	AL	AU	BE	BO	CR	ES	LA	LIT	GE	HU	IT	MO	NO	PO	PO	SE	SL	MA	SW	UR
Specific provisions						√					√									

- Is your legal framework providing for a regulation of Profiling?

	AL	AU	BE	BO	CR	ES	LA	LIT	GE	HU	IT	MO	NO	PO	PO	SE	SL	MA	SW	UR

Specific provisions						√					√								

Few States have implemented provisions in relation to data mining and profiling. In Italy, private entities can mine medical data obtaining the consent from data subject or using irreversibly anonymized data.

3. RFID and wireless communication technologies

- Is your legal framework providing for a regulation of RFID technologies and the transfer of personal data through wireless technologies?

	AL	AU	BE	BO	CR	ES	LA	LIT	GE	HU	IT	MO	NO	PO	PO	SE	SL	MA	SW	UR
No specific regulation	√	√	√	√	√	√	√	√		√	√	√	√	√	√	√	√	√	√	√

- Is RFID applied in hospitals?

	AL	AU	BE	BO	CR	ES	LA	LIT	GE	HU	IT	MO	NO	PO	PO	SE	SL	MA	SW	UR
Yes		√	√		√	√													√	

RFID regulation does not seem to exist yet but are sometimes used by health professionals. For now, only guidelines from some National Data Protection Authorities have been published.

4. Applications (Mobile)

- Is your legal framework providing for a regulation of Apps and Mobile apps?

No, except in Estonia where Apps and Mobile apps with medical purpose are considered as medical devices, regulated by Medical Devices Act, there is no specific regulation for Apps in the concerned States.

- Is it allowed or do institutions use apps to gather medical data?

According to the compilation of replies, apps are used in Croatia, Italy, and Switzerland. Most often, the same rules apply as for other IT equipment's dealing with medical data.

- Is there any requirement to implement privacy by design?

Not in general. In Albania, there are requirement to implement the development of Privacy by design in medical equipment but based on the standards of the medical device (soft law).

5. Medical Devices and Wearable Devices

- Is your legal framework providing for a regulation of Medical Devices?

Not for the concerned member States. However in EU Member States due to EU regulation, all medical devices should wear CE marking of conformity.

- Does the concept of Medical device in your country encompass apps or services and apparels in the realm of eHealth and mHealth?

It appears that eHealth and mHealth devices and apps are not currently considered as medical devices and therefore are not subject to the same requirements.

There are currently no binding rules as to the difference between lifestyle and wellbeing apps and a medical device or in vitro diagnostic medical device. For instance, the only EU legal framework for

now is the Commission's guidelines "on the qualification and classification of stand-alone software used in healthcare within the regulatory framework of medical devices".

Examples of soft law or regulation in that field are rare. In Estonia, apps are considered as medical devices by Ministry of Social Affairs in Estonia. In Austria, identification of medical devices with bar codes is used.

6. Internet of Things

- Is your legal framework providing for a regulation of Internet of Things?

Not in the concerned member States.

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

- Is your legal framework providing for a regulation of online Medical Treatment and in the on-line appointment system covered by such a framework?

Not in the concerned member States.

- Is it allowed to perform medical treatment via online services?

It is generally not allowed.

2. Recapitulation of the proposals

Proposal No. 1

- Define health data broadly to include all information that might characterise an individual's state of health, deliveries of health services provided, and the person's medical welfare environment.

- Define the concepts of "anonymisation" "pseudonymisation".

Proposal No. 2

- Define the concepts of exchanging and sharing health data.

- Define the terms "urbanisation of health information systems" and "interoperability".

Proposal No. 3

- Define the terms hosting/Cloud Computing.

- Define the term "mobile health", distinguishing the wellness from the health care purposes and the data produced by the patient personally and on his/her responsibility from those produced with the intervention of professionals (health and medical welfare sector).

Proposal No. 4

- Recall the major principles of personal health data protection while incorporating, via the "*privacy by design*" principle, the concept of conformity with a framework which permits adjustment as regards the purposes of data gathering and processing and as regards designation of the data controller(s).

- Recognise professional secrecy shared between health professionals caring for the same patients.

Proposal No. 5

- Make the principle of conformity to interoperability reference frameworks enforceable.

- Leave the organisation of their updating to the states.

Proposal No. 6

- Recall the importance of security measures in the handling of health information.

- Make the reference frameworks identifying the players, both professionals and patients, enforceable.

Proposal No. 7

- Strengthen patients' rights over their health data by incorporating the concept of empowerment.

- Limit the recording of consent to cases where domestic law expressly provides for it.

Proposal No. 8

- Adapt to the new context of proliferation of health data the regulatory framework allowing secondary use of such data for purposes of improving public health.