COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 20 September / septembre 2016 T-PD(2016)07MosRev

THE CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA (T-PD)

Compilation of comments received on

DRAFT RECOMMENDATION ON THE PROTECTION OF HEALTH DATA

****

COMITE CONSULTATIF DE LA CONVENTION POUR LA PROTECTION DES PERSONNES A L'EGARD DU TRAITEMENT AUTOMATISE DES DONNEES A CARACTERE PERSONNEL (T-PD)

Compilation de commentaires reçus sur le PROJET DE RECOMMANDATION EN MATIERE DE PROTECTION DES DONNEES DE SANTE

Directorate General / Direction Générale

Human Rights and Rule of Law / Droits de l'Homme et Etat de droit

TABLE / INDEX

AUSTRIA/ AUTRICHE

recommendation CM/Rec(2016)…. of the Committee of Ministers to member States on the protection of health data
(adopted by the Committee of Ministers … 2016,
at the … meeting of the Ministers' Deputies)

[…]

Appendix to Recommendation CM/Rec(2016)…

Chapter I
General provisions

Purpose

The purpose of this Recommendation is to provide member States with guidance for regulating the processing, and the different uses, of health data in order to guarantee respect for the rights and fundamental freedoms of every natural person, particularly the right to privacy. It also provides guidelines for developing interoperable and secured information systems in a manner enabling the quality of care and the efficiency of health systems to be enhanced.

Scope

This Recommendation is applicable to the processing of personal data relating to health (health data) in the public and private sectors.

It also lays down the principles for the exchange and sharing of health data by means of digital tools with due regard for the rights of the individual and the confidentiality of data.

The provisions of this Recommendation do not apply to health data processing performed by individuals in the context of exclusively personal or domestic activities.

Definitions

For the purposes of this Recommendation, the following expressions are defined as follows:

- The expression "personal data" refers to any information relating to an identified or identifiable individual. An individual shall not be regarded as "identifiable" if identification requires an unreasonable amount of time and effort. In cases where the individual is not identifiable, the data are referred to as anonymous.

- The expression "health data" covers all data that may reveal the data subject's past, present or future state of health in relation to his/her physical and/or mental condition, irrespective of their source. It also covers any information relating to his/her health and welfare provision. It may also involve information of a biological and genetic nature. It further covers data relating to well-being and/or lifestyle where these reveal a state of health.

Comment [SM1]: unless otherwise intended the definition of health data should be aligned to the definition used in Art. 4.15 of the EU GDPR (Regulation No. 2016/679)

- The expression "genetic data" refers to any data relating to an individual's genetic characteristics, whether inherited or acquired at an early stage of prenatal development, resulting from the analysis of a biological sample from that individual: analysis of chromosomes, DNA or RNA or any other component making it possible to obtain equivalent information.

Comment [SM2]: unless otherwise intended the definition of genetic data should be aligned to the definition used in Art. 4.13 of the GDPR

- The expression "reference framework" denotes a coordinated set of rules and/or processes kept constantly state-of-the-art and applicable to health information systems, covering the areas of identification, interoperability and security.

- The expression "electronic medical file" denotes a secured set of health data, structured or not, of one individual, which accompanies them throughout the course of their treatment. It enables the patient and authorised health professionals to share the information that is useful for co-ordinating care.

- The expression "secure messaging system" denotes a service for the secure exchange of personal health data between identified individuals.

- The expression "right to portability" denotes a person's right to receive data concerning them that have been entrusted to a data controller, in a structured, commonly used and machine-readable format, and to transmit them without hindrance, if necessary, to another controller.

Comment [SM3]: see Art. 20.1 GDPR

- The expression "mobile applications" denotes a set of means accessible in a mobile environment making it possible to communicate and manage health data remotely. It covers different forms such as connected medical objects and devices.

- The expression “health professionals” covers all professionals recognised as such by national and European Union law practising in the health, medical welfare or social welfare sector, bound by professional secrecy and involved in co-ordinating treatment for an individual to whom they provide health care.

- The expression "health data hosting" denotes the use of third-party agencies for the secure and lasting storage of health data on the Internet.

- The expression "anonymisation" denotes the process applied to health data so that the data subject can no longer be identified, either directly or indirectly. Anonymisation is irreversible.
- The expression "pseudonymisation" denotes a technique whereby data can be made non-identifying for as long as they are not associated with other elements stored separately which would make identification possible.

Comment [SM4]: unless otherwise intended the definition of pseudonymisation should be aligned to the definition used in Art. 4.5 of the GDPR

- The concepts of exchange and sharing of health data, which can be features of health data processing, are defined as follows:

(a) Data exchange is the communication of information to a clearly identified recipient or recipients by a known transmitting party.

(b) Data sharing enables data to be made available to several persons entitled to be made aware of such data according to the principles of the right of access, without these persons necessarily being known at the outset.

- The term communication refers to any processing operation and in particular the exchange or sharing of personal data enabling authorised persons to have access to personal data, regardless of the means or devices used.

Chapter II
The legal conditions for use of health data

Compliance with the principles of personal data protection and Privacy by design

Comment [SM5]: Why solely privacy by design? The principles listed below are common data protection principles. Privacy by design is a technique to implement basic data protection principles (see also para 4.5. and 14 of the present draft).

4.1 Anyone processing health data must comply with the following principles:

a. The processing of data should be proportionate in relation to the legitimate purpose pursued and shall be carried out only on the basis of free, specific, informed and unambiguous consent of the data subject or on other legitimate basis laid down by law.

b. Personal data must be processed lawfully and fairly. They must be collected for explicit, specified and legitimate purposes and must not be processed in a manner that is incompatible with these purposes; subsequent processing for scientific or historical research purposes or statistical purposes is compatible with those purposes on condition that additional guarantees apply.

c. The data must be adequate, relevant and not excessive in view of the purposes for which they are processed; they must be accurate and, if necessary, updated.

d. The data must be stored in a form allowing identification of the data subjects for a period not beyond what is necessary for the purposes for which they are processed.

e. Appropriate security measures must be established to prevent risks such as accidental or unauthorised access to personal data or the destruction, loss, use, modification or disclosure to unauthorised third parties of those data.

f. The rights of the person whose data are collected and processed must be respected, particularly their rights of access to the data, communication, rectification and objection.

4.2 The processing of health data is permissible only insofar as specific and appropriate guarantees are provided for in domestic law to prevent any risk to the interests, rights and fundamental freedoms of the data subject which the processing may represent, in particular the risk of discrimination.

4.3 The purposes for which health data are processed must also be taken into account in order to ensure appropriate use of these data and to adapt the safeguards accordingly.

4.4 In principle, health data must be collected and processed by health professionals, agencies acting under the responsibility of health professionals or by the data subjects themselves. Data controllers and their processors who are not health professionals should only collect and process health data in accordance with the same rules of confidentiality and security measures that apply to health professionals.

4.5 These personal data protection principles must be taken into account and incorporated right from the design of information systems collecting, using and exploiting health data. Compliance with these principles must be regularly reviewed throughout the life cycle of the processing. The controller must assess the impact of the applications used in terms of data protection and respect for privacy.

4.6 The controller must take all appropriate measures to fulfil their obligations with regard to data protection and must be able to demonstrate in particular to the competent supervisory authority that the processing for which they are responsible is in line with those obligations.

5. Processing of health data

5.1 Health data must be processed fairly and lawfully and only for specified purposes.

5.2 Health data shall in principle be collected from the data subject. They may be collected from other sources only if in accordance with principles 5, 6, 7, 9 and 12 of this Recommendation and if this is necessary to achieve the purpose of the processing or if the data subject is not in a position to provide the data.

5.3 Health data may be processed and communicated:

a. if provided for by law or if the processing is based on a contract concluded with a health professional stipulating appropriate safeguards:
   i. for preventive medical purposes and for purposes of medical diagnoses, administration of care or treatment, or management of health services by health professionals and those of the social and medical welfare sector;
   ii. for reasons of public interest in the public health field, such as for example protection against international health hazards or in order to ensure a high standard of quality and safety for medical treatment, health products and medical devices;
   iii. for reasons of public interest in the field of managing claims for social welfare and health insurance benefits and services;
   iv. for reasons of public health provided they are lawful, legitimate and compatible with the initial purpose of the data collection;

b. if the data subject has given his or her consent in accordance with principle 12 of this Recommendation, except in cases where domestic law provides that a ban on processing health data cannot be lifted solely by the data subject's consent;

c. insofar as it is authorised by law:
   i. for purposes of safeguarding the vital interests of the data subject or of a person physically or legally incapable of expressing consent;
   ii. for reasons relating to the obligations of the controllers and to the exercise of their rights or those of the data subject regarding employment and social protection, in accordance with domestic legislation or any collective agreement complying with the said legislation and providing for appropriate safeguards;
   iii. for reasons essential to the recognition, exercise or defence of a legal claim;
   iv. for reasons relating to research in the field of health and the medical welfare sector;
   v. for processing for statistical, historical or scientific research purposes under the conditions defined by domestic law to guarantee protection of the data subject's legitimate interests and where the individual cannot be identified from the results.

In all cases, suitable guarantees must be established to ensure in particular the security of data and respect for the rights of the individual. Any other guarantees may be provided for in domestic law with a view to safeguarding respect for rights and fundamental freedoms.

6. Data concerning embryos and foetuses

6.1 Medical data concerning embryos and foetuses, *inter alia* such as data resulting from a pre-implantation diagnosis, should be considered as personal data and enjoy protection comparable to the protection of the health data of a minor.6.2 Unless otherwise provided for by domestic law, the holder of parental responsibilities may act as the person legally entitled to act in the capacity of data subject.

7. Genetic data

7.1 Genetic data processed with a preventive aim, for diagnosis or for treatment of the data subject or a third person (genetic testing on a legally incapacitated person for the benefit of family members for example) or for scientific research should be used only for these purposes or to enable the data subject to take a free and informed decision on these matters.

7.2 Processing of genetic data for the purpose of a judicial procedure or a criminal investigation should be the subject of a specific law offering appropriate safeguards. The data should be used only to establish whether there is a genetic link in the context of the production of evidence, to prevent a real danger or to punish a specific criminal offence. In no case should they be used to determine other characteristics which may be linked genetically.

7.3 Any processing of genetic data other than in the cases provided for in paragraphs 7.1 and 7.2 should be authorised by the law, particularly where carried out to avoid any serious prejudice to the health of the data subject or third parties. Genetic data may not be used for commercial exploitation in any circumstances. The processing of genetic data in order to predict illness may be authorised in the vital interest and subject to appropriate safeguards provided for by law.

7.4 The publication of genetic data which would identify the data subject, a consanguine or uterine relative of the data subject, a member of his/her social family or a person who has a direct link with his/her genetic line, should be prohibited.

8. Shared medical secrecy for purposes of providing and administering care

8.1 Everyone is entitled to protection of his or her health data. The person receiving care is entitled to respect for his or her privacy and the secrecy of the information concerning them in dealings with a professional operating in the health, medical welfare and social sector.

8.2 In the interests of greater co-ordination between professionals operating in the health and social and medical welfare sector, the domestic law of each member State should recognise a shared

professional secrecy, between professionals who are themselves legally bound by such secrecy.

8.3 The exchange and sharing of data between health professionals must be limited to the information strictly necessary for the co-ordination or continuity of care, prevention or medical welfare-related and social monitoring of the individual, with the respective actors only able to pass on or receive data lying strictly within the scope of their tasks.

8.4 The data subject must be informed beforehand of the nature of the data collected and processed and of the health professionals participating in the care team and must be able to object at any time to the exchange and sharing of his or her health data, save where otherwise provided by domestic law.

Comment [SM6]: there are cases in which the sharing of information is compulsory, e.g. medical data of airline pilots

9. Communication to authorised third parties

9.1 Health data must not be communicated, except in the conditions set out in this Recommendation.

9.2 They may be communicated to third parties where the latter are authorised by domestic law to have ad hoc and limited access to the data. These third parties may be judicial authorities, experts appointed by a court authority or members of staff of an administrative authority designated by an official text.

9.3 Medical officers of insurance companies and employers cannot in principle be regarded as third parties authorised to have access to the health data of patients.

Comment [SM7]:
See para. 11 of the DH-BIO Draft Recommendation on the processing of personal health-related data for insurance purposes, including data resulting from genetic tests:

"Health-related personal data should in principle be collected from the insured person by the insurer. **The transmission of health-related personal data by a third party should be made subject to the insured person's consent."**

Is there a possible contradiction?

Comment [SM8]: There are cases in which employers might have access to medical data of employees, e.g. a nurse or a physician that undergo medical treatment in their hospital; in this case the employer might be authorised to have access to this specific file for administrative purposes (e.g. cost allocation of the treatment)

10. Storage of health data

10.1 Health data should be stored only for the time necessary to achieve the purposes for which they were collected. Domestic law may provide for exact storage periods having regard to the nature of the health data storage medium.

10.2 Storage of health data for other purposes than those for which they were initially collected must be carried out in compliance with the principles of this Recommendation.

10.3 The data subject may personally request deletion of his/her data unless they have been irreversibly rendered anonymous or legitimate interests preclude this.

Chapter III
The rights of the individual

11. Right to information

11.1 Everyone must be informed of the collection and processing of their health data.

They must be informed of:

- the identity and contact details of the controller and of the processors where relevant,
- the purpose for which the data are processed, and where appropriate of the relevant legal basis for it,
- how long the data will be stored,
- the recipients of the data, and planned data transfers to a third country,
- the possibility of refusing the processing of their data, or of withdrawing their initial consent, and the implications of such withdrawal,
- the possibility of their data being subsequently processed for a compatible purpose, in accordance with appropriate safeguards provided for by domestic law,
- the specific techniques used for processing their health data,
- the conditions and the means made available to them for exercising via the controller their rights of access, the right of rectification and deletion of their health data, and the possibility to object to the processing thereof.

Comment [SM9]: "third country" should be defined in an explanatory memorandum because in the current context it is not clear what is meant by this term: A non-EU country? A country not party to Convention 108? A non-member state of the CoE?

11.2 This information should be provided at the time of data collection or of the first communication, unless it proves impossible or requires disproportionate efforts. It must be appropriate and suited to the circumstances. In particular, where the data subject is physically or legally incapable of receiving the information, it may be given to the person legally representing him/her. If a legally incapacitated person is capable of understanding, he/she should be informed before his/her data are processed.

11.3 Information provided to the data subject may be restricted if such derogation is provided for by law and constitutes a necessary and proportionate measure in a democratic society:

- to prevent a real danger or to punish a criminal offence,
- for public health reasons,
- to protect the data subject and the rights and freedoms of others.

11.4 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. In a medical emergency, when the person's life is at stake, care takes precedence over information.

11.5 Domestic law must provide for appropriate safeguards ensuring respect for these rights.

12. Consent

12.1 Where the data subject is required to give his/her consent to the processing of health data, this consent should be free, specific, informed and explicit. When the consent is given digitally, it should be tracked. It does not absolve the person receiving it of the obligations to give prior information.

12.2 The results of genetic analyses should be formulated within the limits of the objectives of the medical consultation, diagnosis or treatment for which consent was obtained.

12.3 Where it is intended to process health data relating to a legally incapacitated person who is incapable of free decision, and where domestic law does not authorise the data subject to act on his/her own behalf, consent is required from the person recognised as legally entitled to act in the interest of the data subject or from an authority or any person or body provided for by law.

12.4 If a legally incapacitated person has been informed of the intention to process his/her health data, his/her wishes should be taken into account, unless domestic law provides otherwise.

13. Right of access, objection rectification, deletion and portability

Comment [SM10]: those rights are mentioned in the substantive part of the text and should therefore also be mentioned in the head-line.

13.1 Everyone must be able to secure access to his or her health data directly from whoever holds them.

13.2 The right of access, implying the right to communication of information, on paper as well, enables the data subject to exercise his/her right of rectification and deletion. It also encompasses the right to receive data in a structured format making it possible to transmit them to another controller designated by the data subject.

13.3 The right of deletion is exercised subject to the cases prescribed by domestic law invoking legitimate grounds. The data subject is entitled to object on legitimate grounds to the collection of his/her personal health data except where the person holding the data invokes an overriding and legitimate reason concerning the public interest of public health.

13.4 If the request to rectify or delete the data is refused or if the data subject's objection is rejected, he or she must be able to challenge this decision before a competent authority.

Comment [SM11]: "appeal" is not a very precise term; see also para. IV.7.7. of the "draft guidelines on the protection of individuals with regard to the processing of personal data in a world of bid data" where the proposed phrase is used.

13.5 Access to health data may be refused, limited or delayed only if the law provides for it and if:

a. this constitutes a necessary and appropriate measure in a democratic society in the interests of protecting national security or public safety, or of preventing, investigating or punishing criminal offences; or
b. knowledge of the information is likely to cause serious harm to the data subject's health;

or

c. the information on the data subject also reveals information on third parties or if, with respect to genetic data, this information is likely to cause serious harm to a consanguine or uterine relative or to a person who has a direct link with this genetic line; or

d. the data are used for scientific or historical research purposes or statistical purposes where there is no identifiable risk of an infringement of the rights and fundamental freedoms of data subjects, in particular where such data are not used for decisions or measures relating to a specific individual.

13.6 The person subjected to genetic analysis should be informed of unexpected findings if the following conditions are met:

a. domestic law does not prohibit the provision of such information;
b. the person himself or herself has asked for this information;
c. the information is not likely to cause serious harm;
   i. to his/her health; or
   ii. to a consanguine or uterine relative, to a member of his/her social family, or to a person who has a direct link with his/her genetic line, unless domestic law provides other appropriate safeguards:

Subject to domestic law, the person should also be informed if this information is of direct importance to him/her for treatment or prevention.

Chapter IV

Reference frameworks for the processing of health data

In the processing of health data all players must observe high standards to ensure the confidentiality of particularly sensitive health data. The possible uses of these data and their disclosure, whether voluntary or not, are potentially highly damaging to an individual. But the issues of data availability (when a critical medical act is to be carried out, for example), integrity and auditability (including traceability) are equally vital.

As the use of digital technology leads to better care, technical considerations take on an ethical dimension, with data availability and interoperability converging with the notion of continuity of care and equality, and technical irreversibility potentially resulting in a loss of opportunity for patients for example.

14. Reference frameworks

14.1 In accordance with the principle of privacy by design as defined in paragraph 4.5, the applications which manage health data must, from their design onwards, incorporate the principles of data protection and the relevant security and interoperability reference frameworks and ensure that the processing of the data complies with these principles and reference frameworks.

14.2 The aim of these reference frameworks is, depending on the use made of data, to define in co-ordination with all the players the conditions governing the use of health data in information systems with a view to ensuring their confidentiality and interoperability. They cover the areas of identification, interoperability and security.

15. Interoperability reference frameworks

15.1 These reference frameworks specify the standards to be used in the exchange or sharing of health data between information systems so that an IT component or system can work together with other existing or future components or systems. They entail using common language (semantic interoperability) and technical reference frameworks (technical interoperability).

15.2 To ensure respect for the rights of data subjects and to enable the development of efficient information systems, health professionals and patients together with any agency authorised to process personal health data, particularly the persons responsible for platforms which allow exchange and sharing of health data, must comply with the security rules and reference frameworks which may be given force of law under each country's domestic law, for example by using a certification process, to be accepted by all players. These rules and reference framework should be complied with particularly where health data are collected and processed in connection with care and treatment.

15.3 The aim of these reference frameworks is to define standards enabling health data to be exchanged and shared by information systems and to monitor their implementation under the conditions of security required.

15.4 They are based on the following principles.

a) using common language and formats of shared or exchanged content based on common standards (semantic interoperability);

b) using interoperable services and common rules on use;

c) using secure interconnection and information delivery protocols for data transport;

d) guaranteeing data subjects reliable identification to ensure the uniqueness of their identity within the different information systems. The identifier chosen must be single, unequivocal, lasting and recognised by all operatives, and founded on a reliable certification system;

e) ensuring authentication of the persons and systems involved in the processing of the data by means of arrangements which all operatives recognise and are such as to guarantee security in the exchange and sharing of the data;

f) using secure solutions as defined in Principle 16.

16. Security reference frameworks

16.1 The processing of health data must be secure and use solutions guaranteeing the availability, integrity, confidentiality and auditability of data.

16.2 These security rules, kept constantly state-of-the-art, should result in the adoption of such technical and organisational measures as to protect personal health data from any illegal or accidental destruction, any loss or any impairment, and to guard against any unauthorised access. In particular, domestic law must make provision for organising and regulating health data collection, storage and restitution procedures.

16.3 System availability– i.e. the proper functioning of the system – must be ensured by measures enabling the data to be made accessible in a secure way and with due regard for each person's permissions.

16.4 Guaranteeing integrity requires verification of every action carried out on the nature of the data, any changes made to or deletion of data, including the communication of data.

16.5 Data confidentiality requires the establishment of measures to monitor access to the data servers and the data themselves, ensuring that only authorised persons are able to access the data.

16.6 Auditability means that there must be a system making it possible to trace any access to the information system and for any action carried out by an individual to be logged to that individual.

16.7 Activity entailing storing health data on the Internet and making them available for users must comply with the security reference framework and principles of personal data protection.

16.8 Professionals who are not directly involved in the person's health care, but by virtue of their assigned tasks ensure the smooth operation of the information systems, may have access, insofar as this is necessary for the fulfilment of their duties and on an ad hoc basis, to personal health data. They must have full regard for professional secrecy and with appropriate measures laid down in domestic law to guarantee the confidentiality and security of the data.

17. Health data management services

17.1 Each member state should establish services for the exchange and sharing of health data as useful aids especially for the co-ordination of care, complying with security and interoperability reference framework defined in sections 14 to 16.

Since these capabilities for exchange and sharing contribute to the quality of care provision and to the proper management of health systems as well as to other goals, for the benefit of both individuals and the collective interest and public health, professionals in the health and social and medical welfare sector should each be equipped for the electronic management of their activity, enabling them to exchange or share personal health data.

17.2 Patients must have the benefit of a secure electronic medical file enabling them to have information useful to their medical, welfare and social monitoring throughout their course of treatment.

The information in this medical file may be shared, with the patient's consent, by professionals involved in care provision for the patient in the conditions defined in paragraph 8.1.

17.3 Any electronic messaging system permitting the exchange of personal health data must comply with the reference framework defined in section 14.

Chapter V
Research in the health field

18. Research in the health field

18.1 The use of health data for the purposes of research in the health field must be carried out with a legitimate aim and in full compliance with the principles laid down in this Recommendation.

18.2 The need to use health data must be evaluated in the light of the aim pursued.

18.3 Persons whose data are being used for research must be informed of such use and, where provided for in domestic law, give their consent, except in cases of medical emergency.

When the data subject is a legally incapacitated person and domestic law does not authorise the data subject to act on his/her own behalf, his/her legal representative or an authority, or any person or body provided for by law, shall be provided with the information and/or shall give his or her consent in the context of the research project.

18.4 The conditions in which health data are processed for research in the health field and, in particular, the value of such data for public health must be assessed by the body or bodies designated by domestic law;

18.5 Subject to additional provisions determined by domestic law, health-care professionals entitled to carry out their own medical research should be able to use the health data which they hold as long as the data subject has been informed of this possibility and has not objected.

18.6 Personal data used for scientific research may not be published in a form which enables the data subjects to be identified, unless they have given their consent for the publication and publication is authorised by domestic law.

In all cases appropriate safeguards must be introduced to ensure in particular data security and respect for the rights of the individual. Any other guarantees may be provided for in domestic law with a view to safeguarding respect for rights and fundamental freedoms.

Chapter VI
Mobile applications

19. Mobile applications

19.1 The development of mobile applications enables both patients and professionals in the health sector and the welfare and social sector to collect health data and process them remotely. This development takes on different forms and covers several categories of applications, themselves pursuing very different goals of use. Ranging from medical applications to "quantified self" applications, connected devices make it possible to quantify and/or evaluate parameters that may reveal a person's state of health and, in certain cases, are used directly to make diagnoses and provide care.

19.2 Where the data collected by these applications may reveal a person's state of health, concern any information regarding their health care and welfare provision and/or are processed in a medical context, they constitute health data. In this connection they must enjoy the same legal protection and confidentiality applicable to other methods of health data processing as defined by the present Recommendation and, where applicable, supplemented by the domestic law of States.

19.3 Well-being or self-measurement applications used solely for the benefit of the individual using them, operated for solely personal reasons and not generating any external communication should not be considered as being subject to the requirements of the present Recommendation. Guidance on the application of data protection principles to the processing of health data by private sector entities in the context of the use of mobile applications is to be provided distinctly from the present Recommendation.

Comment [SM12]: It is questionable whether these tools don't generate information about a data subject in the same way as social networks do (i.e. by linking several information). In the opinion of the Austrian DPA these applications should also be subject to this Recommendation.

BELGIUM / BELGIQUE

Recommandation CM/Rec(2016)…. du Comité des Ministres aux Etats membres en matière de protection des données de santé *(adoptée par le Comité des Ministres … 2016, lors de la … réunion des Délégués des Ministres).*

Les Etats sont aujourd'hui confrontés à des enjeux majeurs liés au traitement de la donnée de santé, dont l'environnement a, depuis l'adoption de la Recommandation n° R (97) 5 relative à la protection des données médicales, considérablement évolué.

Cette évolution est due au phénomène de dématérialisation de la donnée rendu possible par l'informatisation du secteur de la santé et à la multiplication des échanges du fait du développement d'internet.

L'informatisation croissante du secteur professionnel et notamment des activités de soins et de prévention, de recherche en sciences de la vie, de gestion du système de santé, et d'autre part l'implication croissante des patients caractérisent notamment ce nouvel environnement.

En outre, les phénomènes de mobilité, le développement des objets et dispositifs médicaux connectés contribuent à de nouveaux usages et à la production d'un volume rapidement croissant de données.

Ce constat partagé par les Etats membres conduit à proposer une nouvelle rédaction de la Recommandation n° R (97) 5 relative à la protection des données médicales, terme auquel on préfèrera le terme plus général de « données de santé », en réaffirmant le caractère sensible des données de santé et l'importance d'encadrer leur utilisation afin de garantir un usage respectant les droits et libertés fondamentales de l'individu notamment le droit au respect de la vie privée.

Comment [A13]: OK pour nous. Le texte de la Convention 108 modernisée admet une approche téléologique pour les données de santé qui sont qualifiées comme telles dès lors qu'elles sont traitées "pour l'information qu'elle révèle sur la santé". est-ce qu'il ne faudrait pas que la recommandation y fasse écho d'une manière ou d'une autre ? En indiquant que la recommandation part de cet a priori. Ou est-ce l'évidence dès lors que la recommndation porte sur les données de santé.

Le Comité des Ministres, conformément à l'article 15.*b* du Statut du Conseil de l'Europe, recommande aux Etats membres :

– d'assurer que les principes contenus dans l'annexe de la présente recommandation, qui remplace la Recommandation N° R (97) 5 susmentionnée, sont reflétés dans la mise en œuvre des législations nationales relatives à la protection des données de santé, ainsi que dans d'autres branches de toute loi portant sur l'utilisation des données de santé ;

– d'assurer, à cette fin, que la présente recommandation et son annexe sont portées à l'attention des autorités établies conformément à la législation nationale en matière de protection de données et chargées de contrôler l'application de cette législation, ainsi que des autorités en charge des systèmes de santé ;

Comment [A14]: Ajout également des professionels des soins de santé

– de promouvoir l'acceptation et l'application des principes contenus dans l'annexe de la présente recommandation, au moyen d'instruments complémentaires, tels que des codes de conduite, en s'assurant que ces principes sont bien connus, compris et mis en application par tous les intervenants du secteur de la santé, et pris en compte dans la conception, le déploiement et l'utilisation des TIC dans ce secteur.

Annexe à la Recommandation CM/Rec(2016)…

Chapitre I

Dispositions générales

Objet

La présente Recommandation a pour objet de fournir aux Etats membres des orientations en vue d'encadrer l'utilisation et les différents usages des données de santé afin de garantir le respect des droits et libertés fondamentales de toute personne physique notamment le droit à la vie privée. Elle fournit également les lignes directrices d'un développement de systèmes d'information interopérables et sécurisés permettant d'accroitre la qualité des soins et l'efficience des systèmes de santé.

Comment [A15]: Ajouter également la collecte

Champ d'application

La présente recommandation est applicable au traitement de données à caractère personnel relatives à la santé (données de santé) dans les secteurs publics et privés.

Elle définit également les principes de l'échange et du partage des données de santé à l'aide des outils numériques respectueux des droits de la personne et de la confidentialité des données.

Les dispositions de la présente Recommandation ne s'appliquent pas au traitement de données de santé effectué par une personne dans le cadre d'activités exclusivement personnelles ou domestiques.

Définitions

Aux fins de la présente recommandation, les expressions suivantes sont définies ainsi :

- L'expression « donnée à caractère personnel » signifie toute information concernant une personne physique identifiée ou identifiable. Une personne physique n'est pas considérée comme identifiable si cette identification nécessite des délais ou des activités déraisonnables. Lorsqu'une personne physique n'est pas identifiable, les données sont dites anonymes.

- L'expression "données de santé" recouvre toutes données susceptibles de révéler l'état de santé de la personne en relation avec son état physique et/ou mental passé, présent ou futur quelle que soit leur source. Elle concerne également toute information relative à sa prise en charge sanitaire et sociale. Il peut s'agir par ailleurs d'informations de nature biologique et génétique. Sont en outre concernées les données relevant du bien-être et/ou des habitudes de vie dès lors qu'elles révèlent un état de santé.

Comment [A16]: le texte ne précise pas qu'il doit s'agir de données à caractère personnel. Si c'est l'intention , ne faut-il pas l'expliciter davantage. D'autant qu' ensuite le texte parle d'information , ce qui élargit également la portée de la recommandation.

Comment [A17]: Une partie du texte ne devrait-il pas plutôt figurer dans l'exposé des motifs de la recommandation plutôt que dans la "définition"

- L'expression « données génétiques » se réfère à toute donnée relative aux caractéristiques génétiques d'un individu soit héritées soit acquises à un stade précoce du développement prénatal, résultant de l'analyse d'un échantillon biologique de cet individu : analyse des chromosomes, de l'ADN ou de l'ARN ou de tout autre élément permettant d'obtenir des informations équivalentes.

- L'expression "référentiels" désigne un ensemble coordonné de règles et/ou de processus maintenu à l'état de l'art et applicable aux systèmes d'information de santé et qui recouvre les domaines de l'identification, de l'interopérabilité et de la sécurité.

- L'expression "dossier médical électronique" désigne un ensemble sécurisé, structuré ou non, de données de santé d'une même personne qui l'accompagne tout au long de son parcours de soins. Il permet au patient et aux professionnels de santé autorisés de partager les informations utiles à la coordination des soins.

- L'expression "messagerie sécurisée" désigne un service permettant d'échanger de façon sécurisée des données de santé à caractère personnel entre personnes identifiées.

- L'expression "droit à la portabilité " désigne le droit pour les personnes concernées de recevoir les données les concernant confiées à un responsable du traitement, dans un format structuré, et couramment utilisé et de les transmettre, le cas échéant, à un autre responsable du traitement.

- L'expression "applications mobiles" désigne un ensemble de moyens accessibles en mobilité permettant de communiquer et de gérer des données de santé à distance. Elle recouvre des formes diverses comme les objets connectés et les dispositifs médicaux.

- L'expression "professionnels de santé" recouvre tout professionnel reconnu comme tel par le droit national et le droit de l'Union européenne, exerçant dans le secteur sanitaire, médico-social ou social, astreint au secret professionnel et participant à la coordination des soins d'une personne qu'il prend en charge.

Comment [A18]: Ou une obligation de confidentalité/secret équivalente prévue par la loi ?

- L'expression "hébergement de données de santé" désigne le recours à des organismes tiers pour assurer de façon sécurisée et pérenne la conservation de données de santé sur internet.

- L'expression "anonymisation" désigne le procédé appliqué aux données de santé pour que les personnes concernées ne puissent plus être identifiées ni directement, ni indirectement. L'anonymisation est irréversible.

- L'expression "pseudonymisation" désigne une technique qui permet de rendre une donnée non identifiante aussi longtemps qu'elle n'est pas associée à d'autres éléments conservés séparément et qui permettraient une identification.

- Les notions d'échange et de partage de données de santé qui peuvent caractériser le traitement des données de santé sont définies de la façon suivante. L'échange de données correspond à la communication d'informations à un (des) destinataire(s) clairement identifié(s) par un émetteur connu. Le partage de données permet de mettre des données à la disposition de plusieurs personnes fondées à en connaître selon des principes de droit d'accès sans que ces personnes ne soient nécessairement initialement connues.

- Le terme "communication" signifie toute opération de traitement et notamment l'échange ou le partage de données à caractère personnel permettant de rendre accessibles à des personnes autorisées des données à caractère personnel, quels que soient les moyens ou les supports utilisés.

Chapitre II

Les conditions juridiques d'utilisation des données de santé

Le respect des principes de protection des données à caractère personnel dès la conception (privacy by design)

4.1 La personne qui traite des données de santé doit respecter les principes suivants :

a. Le traitement des données doit être proportionné à la finalité légitime poursuivie et ne peut être effectué que sur la base du consentement libre, spécifique, éclairé et non-équivoque de la personne concernée ou en vertu d'autres fondements légitimes prévus par la loi.

b. Les données à caractère personnel doivent être traitées licitement, de façon loyale. Elles doivent être collectées pour des finalités explicites, déterminées et légitimes et ne doivent pas être traitées de manière incompatible avec ces finalités ; le traitement ultérieur à des fins de recherche scientifique ou historique ou à des fins statistiques est compatible avec ces fins, à condition que des garanties complémentaires s'appliquent.

c. Les données doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées ; elles doivent être exactes et si nécessaire mises à jour.

d. Les données doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont traitées.

e. Des mesures de sécurité appropriées doivent être mises en place pour empêcher les risques tels que l'accès accidentel ou non autorisé aux données à caractère personnel, leur destruction, perte, utilisation, modification ou divulgation à des tiers non autorisés.

f. Les droits de la personne dont les données sont collectées et traitées doivent être respectés, en particulier son droit d'accès aux données, de communication, de rectification et d'opposition.

Comment [A19]: Le droit à la portabilité n'est ici pas mentionné. Par contre, il est fait référence à la "communication" , veut-on ici viser l'accès + copie + portabilité ?

4.2 Le traitement de données de santé n'est autorisé que dans la mesure où des garanties spécifiques et appropriées sont prévues par le droit interne afin de prévenir les risques que leur traitement peut présenter pour les intérêts, droits et libertés fondamentales de la personne concernée, notamment un risque de discrimination.

4.3 Les finalités pour lesquelles les données de santé sont traitées doivent également être prises en compte pour permettre un usage pertinent de ces données et adapter en conséquence les garanties.

Comment [A20]: Nous ne comprenons pas bien la simple référence au fait de "prendre en compte" le principe de finalité. N'est-ce pas une évidence ? Les données ne peuvent être traitées que pour les finalités identifiées par le responsable de traitement

4.4 En principe, les données de santé doivent être collectées et traitées par des professionnels de santé, des organismes agissant sous la responsabilité de professionnels de santé ou par les personnes concernées elles-mêmes. Les responsables du traitement et leurs sous-traitants qui ne sont pas des professionnels de santé ne devraient collecter et traiter des données de santé que dans le respect de règles de confidentialité et de mesures de sécurité comparables à celles incombant à un professionnel de santé.

4.5 Ces principes de protection des données personnelles doivent être pris en compte et intégrés dès la conception des systèmes d'information collectant, utilisant et exploitant des données de santé. Le respect de ces principes doit être réexaminé régulièrement tout au long de la vie du traitement. Le responsable du traitement doit évaluer l'impact en termes de protection des données et de respect de la vie privée de ses applications.

4.6 Le responsable du traitement doit prendre toutes les mesures appropriées afin de se conformer à ses obligations en matière de protection des données personnelles et doit être en mesure de démontrer en particulier à l'autorité de contrôle compétente que le traitement dont il est responsable est en conformité avec de telles obligations.

5. Le traitement des données de santé

5.1 Le traitement des données de santé doit être effectué de manière loyale et licite et uniquement pour des finalités déterminées.

5.2 Les données de santé doivent en principe être collectées auprès de la personne concernée. Elles ne peuvent être collectées auprès d'autres sources que conformément aux principes 5, 6, 7, 9 et 12 de la présente recommandation, et à condition que cela soit nécessaire pour réaliser la finalité du traitement ou que la personne concernée ne soit pas en mesure de fournir les données.

5.3 Les données de santé peuvent être traitées et communiquées :

d. si la loi le prévoit ou si le traitement repose sur un contrat avec un professionnel de la santé prévoyant des garanties appropriées :
   v. aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements ou de gestion de services de santé par les professionnels de santé et du secteur social et médico-social ;
   vi. pour des motifs d'intérêt public dans le domaine de la santé publique comme par exemple, la protection à l'égard de risques sanitaires internationaux ou pour assurer un haut niveau de qualité et de sécurité aux traitements médicaux, produits de santé et dispositifs médicaux ;
   vii. pour des motifs d'intérêt général dans le domaine de la gestion des demandes de prestations et de services de protection sociale et d'assurance maladie ;
   viii. pour des motifs de santé publique dès lors qu'ils sont licites, légitimes et sont compatibles avec la finalité initiale de collecte des données ;

e. si la personne concernée a donné son consentement conformément au principe 12 de la présente recommandation, sauf dans les cas où le droit interne prévoit qu'une interdiction de traiter les données de santé ne peut être levée par le seul consentement de la personne concernée ;

f. dans la mesure où la loi l'autorise :
   vi. aux fins de sauvegarde des intérêts vitaux de la personne ou d'une personne incapable physiquement ou légalement d'exprimer son consentement ;
   vii. pour des motifs tenant aux obligations des responsables du traitement et à l'exercice de leurs droits ou de ceux de la personne concernée dans le domaine de l'emploi et de la protection sociale, dans le respect des règles du droit interne ou de tout accord collectif respectueux de ce dernier et prévoyant des garanties appropriées ;
   viii. pour des motifs nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice
   ix. pour des motifs tenant à la recherche dans le domaine de la santé et du secteur médico-social ;
   x. pour des traitements à des fins de recherche scientifique ou historique ou à des fins statistiques dans les conditions définies par le droit interne pour garantir la protection des intérêts légitimes de la personne et dès lors que le résultat ne permet pas d'identifier la personne.

Comment [A21]: Pour la bonne compréhension de tous, l'exposé des motifs pourrait expliciter la distinction que'opère la recommandation entre "prévu par la loi / provided by law" et 'autorisé par la loi".

Dans tous les cas, des garanties appropriées doivent être mises en place pour assurer en particulier la sécurité des données et le respect des droits de la personne. Toute autre garantie peut être prévue par le droit interne afin de garantir le respect des droits et libertés fondamentales.

Données relatives à l'embryon et au fœtus

6.1 Les données médicales relatives à l'embryon et au fœtus, telles que notamment les données résultant d'un diagnostic préimplantatoire, devraient être considérées comme des données à caractère personnel relatives à la santé et jouir d'une protection comparable à celle des données de santé d'un mineur.

Formatted: Highlight

6.2 A moins que le droit interne n'en dispose autrement, le détenteur des responsabilités parentales peut agir en qualité de personne habilitée juridiquement à agir en tant que personne concernée.

Données génétiques

Comment [A22]: Attention, dans la définition de donnée de santé, le texte évoque des informations de nature génétique. Or ici on a une disposition spécifique consacrée aux données génétiques avec des bases de légitimité propre. Par exemple, il semble que le consentement/contrat soit exclu ici sauf à prévoir que la loi l'autorise ? En application de la loi belge, le consentement est exclu par exemple pour la transmission de données génétiques à des compagnies d'assurance (interdiction même si consentement prévue par la loi sur les assurances terrestres)

7.1 Les données génétiques traitées à des fins de prévention, de diagnostic, ou à des fins thérapeutiques à l'égard de la personne concernée ou d'une tierce personne (tests génétiques sur des incapables au bénéfice de membres de leur famille par exemple) ou pour la recherche scientifique ne devraient être utilisées qu'à ces seules fins ou pour permettre à la personne concernée de prendre une décision libre et éclairée à leur sujet.

7.2 Le traitement des données génétiques pour les besoins d'une procédure judiciaire ou d'une enquête pénale devrait faire l'objet d'une loi spécifique offrant des garanties appropriées. Ces données devraient servir exclusivement à la vérification de l'existence d'un lien génétique dans le cadre de l'administration de la preuve, à la prévention d'un danger concret ou à la répression d'une infraction pénale déterminée. En aucun cas elles ne devraient être utilisées pour déterminer d'autres caractéristiques qui peuvent être liées génétiquement.

7.3 Tout traitement des données génétiques à d'autres fins que celles prévues aux points 7.1 et 7.2 devrait être autorisé par la loi, en particulier dans les cas où il s'agit de prévenir un préjudice sérieux pour la santé de la personne concernée ou de tiers. En aucun cas, les données génétiques ne peuvent donner lieu à une exploitation commerciale. Le traitement des données génétiques en vue de dépister des maladies peut être autorisé dans l'intérêt vital et dès lors qu'il existe des garanties appropriées définies par la loi.

7.4 La publication de données génétiques permettant d'identifier la personne concernée, un parent consanguin ou utérin de la personne concernée, un membre de sa famille sociale, ou une personne ayant un lien direct avec la lignée génétique de la personne concernée devrait être interdite.

Le secret médical partagé aux fins de prise en charge et d'administration des soins

8.1 Toute personne a droit à la protection de ses données de santé. Dans le cadre de ses relations avec un professionnel de santé, médico-social et social, la personne prise en charge a droit au respect de sa vie privée et au secret des informations la concernant.

8.2 La nécessité d'une plus grande coordination entre professionnels intervenant dans le secteur sanitaire, médico-social et social doit conduire le droit interne de chacun des Etats membres à

reconnaitre un secret professionnel partagé entre des professionnels eux-mêmes astreints au secret professionnel par la loi.

8.3. L'échange et le partage de données de santé entre professionnels de santé doivent être limités aux informations strictement nécessaires à la coordination ou la continuité des soins, à la prévention ou au suivi médico-social et social de la personne, chacun ne pouvant transmettre ou recevoir que les données qui relèvent strictement du périmètre de ses missions.

8.4 La personne concernée doit être informée préalablement de la nature des données collectées et traitées et des professionnels de santé participant à l'équipe de soins. Elle doit pouvoir à tout moment s'opposer à l'échange et au partage de ses données de santé.

Communication à des tiers autorisés

9.1 Les données de santé ne doivent pas être communiquées, sauf dans les conditions énumérées dans le cadre de la présente Recommandation.

9.2 Elles peuvent être communiquées à des tiers autorisés par le droit interne à obtenir un accès ponctuel et limité aux données. Il peut s'agir des autorités judiciaires, des experts désignés par une autorité juridictionnelle ou des agents d'une administration désignés par un texte.

9.3 Les médecins de compagnies d'assurance et les employeurs ne peuvent être considérés comme des tiers autorisés à accéder aux données de santé des patients.

La conservation des données de santé

10.1 Les données de santé ne doivent être conservées que pour la durée nécessaire à la réalisation des finalités pour lesquelles elles ont été collectées. Le droit interne peut prévoir des durées de conservation précises tenant compte de la nature du support de conservation des données de santé.

10.2 La conservation de données de santé pour des finalités différentes de celles pour lesquelles elles ont été initialement collectées, doit être réalisée dans le respect des principes de la présente Recommandation.

10.3 La personne concernée peut elle-même demander la suppression de ses données à moins qu'elles ne soient rendues anonymes de façon irréversible ou que des intérêts légitimes s'y opposent.

Comment [A23]: Dans ce cas, il ne s'agit plus de données personnelles et rien ne s'oppose à la conservation de données anonymisées

Chapitre III

Les droits de la personne

Le droit à l'information

11.1 Toute personne doit être informée de la collecte et du traitement de ses données de santé.

Elle devrait être informée :

- de l'identité et des coordonnées du responsable du traitement et, le cas échéant, de celle de ses sous-traitants,
- de la finalité du traitement des données et de l'existence, le cas échéant, de son fondement légal,
- de la durée de conservation de ses données,
- des destinataires des données et des transferts de données prévus vers un pays tiers,
- de la possibilité de refuser le traitement de ses données ou de revenir sur son accord initial et des conséquences qui s'y attachent,
- de la possibilité de traiter ultérieurement ses données pour une finalité compatible dans le respect de garanties appropriées prévues par le droit interne,
- des techniques particulières utilisées pour traiter ses données de santé,
- des conditions et des moyens mis à sa disposition pour exercer auprès du responsable du traitement ses droits d'accès, de rectification et de suppression de ses données de santé et de la possibilité de s'opposer à leur traitement.

Comment [A24]: Suggestion d'ajouter un point de contact, DPO par exemple pour anticiper la Convention modernisée/rappprt explicatif qui mentionne la possibilité de désigner un DPO qui serait particulièrement le bienvenu dans le secteur de la santé

Comment [A25]: Ici aussi cela devrait être explicité dans l'exposé des motifs de la recommandation pour mettre en évidence la valeur ajoutée de cet élément d'information à la personne concernée

11.2 Cette information doit être réalisée au moment de la collecte des données ou lors de la première communication à moins que cette information se révèle impossible ou exige des efforts disproportionnés. Elle doit être appropriée et adaptée aux circonstances. En particulier, lorsque la personne est dans l'incapacité physique ou juridique de recevoir cette information, celle-ci pourra être donnée à la personne qui la représente légalement. Si elle est en mesure de comprendre, la personne légalement incapable devrait être informée avant que les données qui la concernent soient traitées.

11.3 L'information de la personne concernée peut être limitée, si la dérogation est prévue par la loi et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique :

- à la prévention d'un danger concret ou à la répression d'une infraction pénale,
- pour des raisons de santé publique,
- pour protéger la personne et les droits et libertés des tiers.

11.4 La volonté d'une personne d'être tenue dans l'ignorance d'un diagnostic ou d'un pronostic doit être respectée, sauf lorsque des tiers sont exposés à un risque de transmission. En cas d'urgence médicale, lorsque la vie de la personne est en jeu, les soins priment sur l'information.

Comment [A26]: Préciser qu'il s'agit d'une transmission au sens médical ? Et non pas une communication des données à des tiers. C'est à tout le moins la manière dont nous comprenons le §.

11.5 Le droit interne doit prévoir les garanties appropriées de nature à assurer le respect de ces droits.

Le consentement

12.1 Lorsque la personne concernée est appelée à donner son consentement au traitement de données de santé, celui-ci devrait être libre, spécifique, éclairé et explicite. Son recueil dès lors qu'il est dématérialisé doit être tracé. Il n'exonère pas celui qui le recueille de ses obligations d'information préalable.

12.2 Les résultats des analyses génétiques devraient être formulés dans les limites des objectifs de la consultation médicale, du diagnostic ou du traitement pour lesquels le consentement a été obtenu.

12.3 Lorsque l'on envisage de traiter des données de santé concernant une personne légalement incapable qui n'est pas en mesure de se déterminer librement, et lorsque le droit interne ne permet pas à la personne concernée d'agir en son propre nom, le consentement de la personne pouvant agir légalement au nom de la personne concernée, ou d'une autorité, ou de toute personne ou instance désignée par la loi, est requis.

12.4 Si la personne légalement incapable a été informée de l'intention de traiter ses données de santé, son souhait devrait être pris en considération, à moins que le droit interne ne s'y oppose.

Le droit d'accès, d'opposition et de portabilité

13.1 Toute personne doit pouvoir accéder à ses données de santé directement auprès de la personne qui les détient.

13.2 Le droit d'accès qui emporte le droit de communication des informations, également sur support papier, permet à la personne d'exercer son droit de rectification et d'effacement. Il emporte avec lui le droit de recevoir les données dans un format structuré qui permette de transmettre les données à un autre responsable de traitement désigné par la personne dont les données sont concernées.

13.3 Le droit à l'effacement s'exerce sous réserve des cas prévus par le droit interne invoquant des motifs légitimes. La personne a le droit de s'opposer pour des motifs légitimes à la collecte de ses données de santé à caractère personnel sauf lorsque le détenteur des données invoque une raison impérieuse et légitime qui concerne l'intérêt général de la santé publique.

13.4 En cas de refus de rectifier ou d'effacer les données ou en cas de rejet de l'opposition de la personne concernée, celle-ci doit pouvoir faire recours.

13.5 L'accès aux données de santé peut être refusé, limité ou différé uniquement si la loi le prévoit, et :

a. si cela constitue une mesure nécessaire et appropriée dans une société démocratique à la protection la sécurité nationale, à la sûreté publique, à la prévention, à l'investigation ou à la répression des infractions pénales ; ou
b. si la connaissance de ces informations est susceptible de causer une atteinte grave à la santé de la personne concernée ; ou
c. si l'information sur la personne révèle également des informations sur des tiers, ou, en ce qui concerne les données génétiques, si ces informations sont susceptibles de porter une atteinte grave à des parents consanguins ou utérins, ou à une personne ayant un lien direct avec cette lignée génétique ; ou
d. si les données sont utilisées à des fins de recherche scientifique ou à des fins statistiques et qu'il n'existe aucun risque identifiable d'atteinte aux droits et libertés fondamentales des personnes concernées, notamment du fait que les données ne sont pas utilisées pour des décisions ou des mesures relatives à une personne déterminée.

13.6 La personne soumise à une analyse génétique devrait être informée des découvertes inattendues si les conditions suivantes ont été remplies :

a. le droit interne n'interdit pas une telle information ;
b. la personne a fait la demande explicite de cette information ;
c. l'information n'est pas susceptible de porter une atteinte grave :
   i. à la santé de la personne ; ou
   ii. à un parent consanguin ou utérin de la personne, à un membre de sa famille sociale, ou à une personne ayant un lien direct avec la lignée génétique de la personne, à moins que le droit interne ne prévoie d'autres garanties appropriées.

Sous réserve du droit interne, la personne devrait également être informée si ces découvertes revêtent pour elle une importance thérapeutique ou préventive directe.

Chapitre IV

Référentiels pour le traitement des données de santé

Comment [A27]: Obtention d'une copie ne serait-il pas plus clair ?

Comment [A28]: Il convient selon nous d'être attentif à ne pas donner l'impression qu'il n'y aurait jamais aucun risque dès lors que les données ne sont pas utilisées pour des données décisions ou mesures relatives à une personne. De plus, dès lors que la disposition porte sur le traitement de données à des fins de recherche ou statistique, il ne peut en principe y avoir de décision individuelle.

Comment [A29]: cumulatives ?

Comment [A30]: A expliciter dans l'exposé des motifs ? Lié à la définition large de données de santé aux termes de cette recommandation.

Comment [A31]: Suggestion d'indiquer que les référentiels sont "sans préjudice de l'application des dispositions légales applicables".

Le traitement des données de santé doit conduire chaque acteur à un niveau d'exigence élevé pour assurer la confidentialité des données de santé particulièrement sensibles.

Les usages qui peuvent en être faits et leur divulgation volontaire ou non exposent les personnes à des préjudices particulièrement importants. Les questions de disponibilité des données (au moment d'un acte médical critique pas exemple), d'intégrité et d'auditabilité (dont l'imputabilité) sont par ailleurs tout aussi essentielles.

Dès lors que le recours au numérique conduit à être mieux soigné, ces considérations techniques deviennent éthiques, la disponibilité des données et l'interopérabilité rejoignant la notion de continuité des soins et d'égalité, une absence de réversibilité technique pouvant se traduire en perte de chance pour le malade par exemple.

Comment [A32]: Le texte devrait être clarifé car il donne l'impression que l'on introduit une distinction entre les données de santé (sensibles et celles qui le seraient moins). Ou l'idée est-elle de rappeler leur nature sensible et ce degré d'exigeance s'applique à toute donnée de santé?.

Référentiels

14.1 Conformément au principe de *privacy by design* tel que défini au point 4.5, les applications qui gèrent des données de santé doivent intégrer dès leur conception les principes de protection des données personnelles et les référentiels de sécurité et d'interopérabilité et s'assurer de la conformité de leur traitement à ces principes et référentiels.

14.2 Ces référentiels ont pour objet, en fonction des usages, de définir de façon coordonnée avec les acteurs les conditions d'usages des données de santé dans les systèmes d'information afin d'assurer leur confidentialité et leur interopérabilité. Ils recouvrent les domaines de l'identification, de l'interopérabilité et de la sécurité.

Les référentiels d'interopérabilité

15.1 Ces référentiels spécifient les standards à utiliser dans les échanges et lors du partage des données de santé entre systèmes d'information de telle façon qu'un produit ou un système informatique puisse fonctionner avec d'autres produits ou systèmes existants ou futurs. Ils impliquent l'utilisation d'un langage commun (interopérabilité sémantique) et des référentiels techniques (interopérabilité technique) communs.

15.2 Pour garantir aux personnes concernées le respect de leurs droits et permettre le développement de systèmes d'information efficients, les professionnels de santé et les patients ainsi que tout organisme autorisé à traiter des données de santé, notamment les personnes responsables des plateformes permettant l'échange et le partage des données de santé, doivent respecter des règles de sécurité et des référentiels auxquels le droit interne de chaque pays peut donner une force juridique par exemple en recourant à un procédé de certification et qui doit conduire à leur acceptabilité par l'ensemble des acteurs. Leur respect doit en particulier être assuré, dès lors que les données de santé sont collectées et traitées dans le cadre des relations de prise en charge et de soins.

15.3 Ces référentiels ont pour objet de définir des standards permettant l'échange et le partage des données de santé par les systèmes d'information et d'assurer le suivi de leur mise en œuvre dans des conditions de sécurité requises.

15.4 Ils sont fondés sur les principes suivants :

a. utiliser un langage et des formats communs de contenus partagés ou échangés fondés sur des standards communs (interopérabilité sémantique) ;

b. recourir à des services interopérables et à des règles d'utilisation communes ;

c. utiliser pour le transport des données, des protocoles d'interconnexion et d'acheminement de l'information sécurisés ;

d. garantir aux personnes concernées une identification fiable afin d'assurer l'unicité de leur identité au sein des différents systèmes d'information. L'identifiant retenu doit être unique, univoque, pérenne et reconnu par l'ensemble des acteurs et fondé sur un dispositif de certification fiable ;

e. assurer l'authentification des personnes et des systèmes qui interviennent dans le traitement des données à l'aide de dispositifs reconnus par l'ensemble des acteurs et de nature à garantir la sécurité de l'échange et du partage des données ;

f. utiliser des solutions sécurisées telles que définies au Principe 16.

Les référentiels de sécurité

16.1 Le traitement des données de santé doit être sécurisé et recourir à des solutions qui garantissent la disponibilité, l'intégrité, la confidentialité et l'auditabilité des données.

16.2 Ces règles de sécurité, maintenues à l'état de l'art, doivent se traduire par l'adoption de mesures techniques et organisationnelles de nature à protéger les données de santé contre toute destruction illégale ou accidentelle, toute perte, toute altération et de prévenir tout accès non autorisé. En particulier, le droit interne doit prévoir d'organiser et d'encadrer les modalités de collecte, de conservation et de restitution des données de santé.

16.3 La disponibilité - c'est-à-dire le bon fonctionnement du système - doit être assurée par des mesures de nature à rendre accessibles les données de façon sécurisée et dans le respect des habilitations de chacun.

16.4 Le respect de l'intégrité impose de vérifier toute action effectuée sur la nature des données, leur modification éventuelle et leur effacement, y compris lors de la communication des données.

16.5 La confidentialité des données se traduit par la mise en place de mesures destinées à contrôler les accès aux serveurs de données et aux données elles-mêmes en s'assurant que seules les personnes autorisées puissent accéder aux données.

16.6 L'auditabilité doit conduire à disposer d'un système permettant de tracer tous les accès au système d'information et de pouvoir imputer à une personne les actions qu'elle a effectuées.

16.7 L'activité qui consiste à conserver sur internet des données de santé et les rendre disponibles pour le compte des utilisateurs doit être réalisée dans le respect des référentiels de sécurité et des principes de protection des données personnelles.

16.8 Des professionnels non impliqués directement dans la prise en charge sanitaire de la personne mais assurant au titre de leurs missions le bon fonctionnement des systèmes d'informations, peuvent accéder dans la mesure indispensable à l'accomplissement de leurs tâches et de façon ponctuelle aux données de santé. Ils doivent respecter le secret professionnel et toutes mesures appropriées prévues par le droit interne pour garantir la confidentialité et la sécurité de ces données.

Les services de gestion des données de santé

17.1 Chaque Etat membre devrait mettre en place les services d'échange et de partage des données de santé, supports utiles en particulier à la coordination des soins et respectueux des référentiels définis aux principes 14 à 16. Dès lors que ces capacités d'échange et de partage contribuent à la qualité des prises en charge comme à la bonne gestion des systèmes de santé et autres finalités, au service tant des individus que de l'intérêt général et de la santé publique, chaque professionnel de santé et du secteur médico-social et social doit disposer d'un dispositif de gestion dématérialisée de son activité le mettant en capacité d'échanger ou de partager les données de santé des personnes.

17.2 Les patients doivent pouvoir bénéficier d'un dossier médical électronique sécurisé qui leur permet de disposer des informations utiles à leur suivi médical, médico-social et social tout au long de leur parcours de soin. Les informations de ce dossier médical peuvent avec l'accord du patient être partagées par les professionnels intervenant dans la prise en charge de la personne dans les conditions définies au principe 8.

Comment [A33]: N'est-ce pas contradictoire d'exiger le consentement du patient dans le cadre du secret partagé ? N'y a t'il pas des cas où, dans l'intérêt (vital) du patient, un accès à d'autres professionnels des soins de santé est admissible ? Par exemple parce que le patient a une relation thérapeutique avec ce professionnel ? Il est à la fois exact qu'il faut distinguer consentement à la relation thérapeutique et consentement aux traitements de données et que tous les professionnels de santé - même dans le cadre de leur relation avec le patient - ne doivent pas avoir accès à toutes les informations. Mais n'est-ce pas là plutôt de la responsabilité /obligation dans le chef des professionnels des soins de santé plutôt que du ressort du consentement du patient ?

17.3 Tout système de messagerie électronique permettant l'échange de données de santé doit respecter les référentiels définis dans le présent Chapitre.

Chapitre V

La recherche dans le domaine de la santé

La recherche dans le domaine de la santé

18.1 L'utilisation des données de santé à des fins de recherche scientifique dans le domaine de la santé devrait être effectuée dans un but légitime et dans le respect des principes posés dans la présente Recommandation.

Comment [A34]: Licite ?

18.2 La nécessité du recours à des données de santé doit être appréciée au regard de la finalité poursuivie.

18.3 Les personnes concernées par la recherche doivent être informées de l'usage de leurs données et, quand le droit national le prévoit, consentir à cet usage sauf en cas d'urgence sanitaire. Lorsque la personne concernée est légalement incapable et que le droit interne ne lui permet pas d'agir en son propre nom, son représentant légal ou une autorité, ou toute personne ou instance désignée par la loi, recevra l'information et/ou donnera son consentement dans le cadre du projet de recherche.

Comment [A35]: Urgence sanitaire ? Dans ce cas, la base de légitimité sera t'elle la recherche ? L'intérêt public ne sera t'il pas davantage invoqué comme base de légitimité ? A expliciter dans l'exposé des motifs de la recommandation

18.4 Les conditions de traitement des données de santé à des fins de recherche dans le domaine de la santé et en particulier leur intérêt pour la santé publique doivent être appréciées par un ou plusieurs organismes désignés par le droit interne.

18.5 Sous réserve de conditions complémentaires prévues par le droit interne, les professionnels de santé habilités à mener leurs propres recherches médicales devraient pouvoir utiliser les données de santé qu'ils détiennent pour autant que la personne concernée ait été informée de cette faculté et ne s'y soit pas opposée.

18.6 Les données à caractère personnel utilisées à des fins de recherche scientifique ne peuvent être publiées sous une forme permettant d'identifier les personnes concernées à moins que ces dernières n'aient donné leur consentement en vue de la publication et que le droit interne autorise cette publication.

Dans tous les cas, des garanties appropriées doivent être mises en place pour assurer en particulier la sécurité des données et le respect des droits de la personne. Toute autre garantie peut être prévue par le droit interne afin de garantir le respect des droits et libertés fondamentales.

Chapitre VI

Les dispositifs mobiles

Les dispositifs mobiles

19.1 Le développement d'applications mobiles permet aux personnes concernées comme aux professionnels du secteur de la santé et du secteur médico-social et social de collecter et traiter à distance des données de santé. Ce développement revêt des formes diverses et recouvre plusieurs catégories d'applications qui elles-mêmes poursuivent des finalités d'usage très différentes. Du dispositif médical aux applications de "mesure de soi" (*quantified self*), ces objets connectés permettent de quantifier et/ou d'évaluer des paramètres susceptibles de révéler l'état de santé d'une personne et sont dans certains cas utilisés directement pour poser des diagnostics et délivrer des soins.

19.2 Dès lors que les données collectées par ces applications sont susceptibles de révéler l'état de santé d'une personne, concernent tout information relative à sa prise en charge sanitaire et sociale et/ou sont traitées dans un contexte médical, elles constituent des données de santé. A ce titre elles doivent bénéficier des mêmes protections juridiques et de confidentialité que celles applicables aux autres modes de traitements de données de santé telles que définies par la présente Recommandation et, le cas échéant, complétées par le droit des Etats.

19.3 Les applications de bien-être ou de "mesure de soi" utilisées pour le seul bénéfice de la personne qui l'utilise, mises en œuvre à des fins exclusivement personnelles et qui ne donnent pas lieu à une communication extérieure ne devraient pas être considérées comme soumises aux exigences de la présente Recommandation. Des orientations sur l'application des principes de protection des données au traitement de données de santé, au moyen de ces applications mobiles, par des entités du secteur privé sont à prévoir dans un document distinct de la présente Recommandation.

DENMARK/ DANEMARK

Denmark notes with approval that Recommendation No. R (97)5 on the protection of medical data is replaced with a more up to date opinion on the matter.

However, it is of great importance to Denmark to find the right balance between protecting the individual's right to protection of their health data and the possibility of register-based research in the health field is found. Denmark consequently proposes a change of the wording of paragraph 18.3 on research in the health field. The paragraph should read as follows (below):

18.3 Persons whose data are being used for research must in general be informed of such use unless it requires disproportionate efforts to inform each individual person. Information about the research project and purpose should in such cases, however, still be provided publically in order to ensure transparency regarding the use of health care data. Persons whose data are being used for research must, where provided for in domestic law, give their consent, except in cases of medical emergency.

* * *

ESTONIA / ESTONIE

Estonian Data Protection Inspectorate has the following comments to the draft recommendation on the protection of health data.

1. **Articles 13.5 and 13.6**, the following wording has been proposed for the experts to consider.

Access to health data (genetic data) may be refused, limited or delayed only if the law provides for it and if this may: - damage rights and freedoms of other persons; - endanger the protection of the confidentiality of filiation of a child; - hinder the prevention of a criminal offence or apprehension of a criminal offender; - complicate the ascertainment of the truth in a criminal proceeding.

2. Article 18.3

Having read the draft recommendation, one might get the idea that patients in cases of medical emergency have fewer possibilities to protect their rights.

3. **Article 18.5**, the following amendment has been proposed:

Subject to additional provisions determined by domestic law, health-care professionals entitled to carry out their own medical research should be able to use the health data which they hold as long as the data subject has prior to processing been informed of this possibility and has not objected.

Furthermore, we would stress the necessity to promote self-auditing tools as health data is highly sensitive and misuse of such data poses high risk to data subjects.

* * *

GERMANY / ALLEMAGNE

Recommendation CM/Rec(2016)…. of the Committee of Ministers to member States on the protection of health data

(adopted by the Committee of Ministers … 2016,

at the … meeting of the Ministers' Deputies)

States face major challenges today, relating to the processing of health data, which now takes place in an environment that has changed considerably since the adoption of Recommendation No. R (97)5 on the protection of medical data.

This changed environment is due to the phenomenon of data digitisation, made possible by the computerisation of the health sector and to the proliferation of exchanges arising from the development of the Internet.

Noteworthy features of this new environment are the growing computerisation of the professional sector and particularly of activities relating to care and prevention, to life sciences research and to health system management, and also the increasing involvement of patients.

Besides, mobility and the development of connected medical objects and devices contribute to new uses and to the production of a rapidly growing volume of data.

This assessment shared by the member States has prompted to propose a revision of Recommendation No. R (97) 5 on the protection of medical data, with the more general term "health data" being preferred, while reaffirming the sensitivity of health data and the importance of regulating their use so as to guarantee due regard for the rights and fundamental freedoms of the individual, in particular the right to privacy.

The Committee of Ministers, under the terms of Article 15.b of the Statute of the Council of Europe, recommends that the member States:

- *take steps to ensure that the principles set forth in the appendix to the present Recommendation, which replaces Recommendation No. R (97) 5 mentioned above, are reflected in their law and practice ~~implementation of national legislation on protection of health data, as well as in other branches of any law on the use of health data~~;*

- *ensure, to that end, that the present Recommendation and its appendix are brought to the attention of the data protection supervisory authorities ~~set up under national data protection legislation to monitor the application of that legislation~~, as well as of the authorities responsible for healthcare systems;*

- *promote acceptance and application of the principles set forth in the appendix to the present Recommendation, using additional instruments such as codes of conduct, while ensuring that these principles are well-known, understood and applied by all the players ~~in the healthcare sector~~processing health data and taken into account in the design, deployment and use of the respective ICTs ~~in that sector~~.*

Comment [BMG36]: Please define "medical objects". The term is not widely used and known. What is the difference between medical objects and medical devices?

Comment [BMG37]: There is a substantial difference between medical data (i.e. data processed for medical purposes by health care professionals) and health data (data concerning the past, current or future state of health irrespective of the profession), or "data concerning health" in accordance with Art. 4 (15) of the GDPR. Whatever term is used, it must be ensured that the broader scope of the recommendation does not dilute the specific data protection regime applied to health care professionals.

Comment [BMG38]: In accordance with Recommendation No. R (97) 5. The protection of medical/health data should not be limited to legislation on the protection or use of health data. Clear language is preferable.

Comment [BMG39]: Recommendation s on the "protection of health data" should not be limited to the healthcare sector. Otherwise the name should be changed into "Recommendations on the protection of personal data in the healthcare sector"

Appendix to Recommendation CM/Rec(2016)…

Chapter I

General provisions

1. Purpose

The purpose of this Recommendation is to provide member States with guidance for regulating the processing, and the different uses, of health data in order to guarantee respect for the rights and fundamental freedoms of every natural person, particularly the right to privacy. It also provides guidelines for developing interoperable and secured information systems in a manner enabling the quality of care and the efficiency of health systems to be enhanced.

2. Scope

This Recommendation is applicable to the processing of personal data ~~relating to~~concerning health (health data) in the public and private sectors, unless domestic law provides other appropriate and equivalent safeguards..

It also lays down the principles for the exchange and sharing of health data by means of digital tools with due regard for the rights of the individual and the confidentiality of data.

The provisions of this Recommendation do not apply to health data processing performed by individuals in the context of exclusively personal or domestic activities.

3. Definitions

For the purposes of this Recommendation, the following expressions are defined as follows:

- The expression "personal data" refers to any information relating to an identified or identifiable individual. An individual shall not be regarded as "identifiable" if identification requires an unreasonable amount of time and effort. In cases where the individual is not identifiable, the data are referred to as anonymous.

- The expression "data concerning health~~ data~~" covers all data that may reveal the data subject's past, present or future state of health in relation to his/her physical and/or mental condition, irrespective of their source. It also covers any information relating to his/her health and welfare provision. It may also involve information of a biological and genetic nature. It further covers data relating to well-being and/or lifestyle where these reveal a state of health.

- The expression "genetic data" refers to any ~~health~~ data concerning health relating to an individual's genetic characteristics, whether inherited or acquired ~~at an early stage of~~ during prenatal development, resulting from the analysis of a biological sample from that individual: analysis of chromosomes, DNA or RNA or any other component making it possible to obtain equivalent information.

- The expression "reference framework" denotes a coordinated set of rules and/or processes kept constantly state-of-the-art and applicable to health information systems, covering the areas of identification, interoperability and security.

- The expression "electronic ~~medical file~~patient summary" denotes a secured set of health data, structured or not, of one individual, which accompanies them throughout the course of their treatment.

Comment [BMG40]: What are "different uses" and how do they relate to "processing"? Wouldn't it be necessary to define processing or delete the wording "and the different uses"?

Comment [BMG41]: It is urgently necessary to examine the need to limit the scope, as in Art. 2 of the General Data Protection Regulation (GDPR).

Comment [BMG42]: In accordance with Art. 4 (15) GDPR

Comment [BMG43]: "in the course of a purely personal or household activity" in accordance with Art. 2 (1) (c) GDPR

Comment [BMG44]: Align with definitions in the GDPR, Art. 4 (1)

Comment [BMG45]: Please use the definitions to explain the differences between the following terms and why they are used in which situation:
- health data and medical data
- medical objects and medical devices
- care and healthcare,
- healthcare sector and health sector,
- medical welfare, social welfare and social protection

Comment [BMG46]: There should also be a definition of "processing" aligned to the GDPR

Comment [BMG47]: Align with Art. 4 (1) GDPR,
"'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;"

Comment [BMG48]: In accordance with Art. 4 (15) GDPR

Comment [BMG49]: align definition with Art. 4 (15) GDPR
"'data concerning health' means personal data related to the physical or mental health of a natural person, including the provisi…

Comment [BMG50]: "social security", in accordance with the GDPR

Comment [BMG51]: The recommendation shall cover health data. Consequently, genetic data covered by this recommendation need to be health relate…

Comment [BMG 252]: See above

Comment [BMG53]: Early stage

Comment [WU54]: This definition is not aligned to the GDPR. For legal clarity, please delete "early stage", as it is not defined when "early stage" of…

Comment [BMG55]: better "patient summary" in accordance with Art. 14 (2) 2011/24/EU

It enables the patient and authorised health professionals to share the information that is useful for co-ordinating care.

- The expression "secure messaging system" denotes a service for the secure exchange of personal health data between identified individuals.

- The expression "right to portability" denotes a person's right to receive data concerning them that have been entrusted to a data controller, in a structured, commonly used format, and to transmit them, if necessary, to another controller.

- The expression "mobile applications" denotes a set of means accessible in a mobile environment making it possible to communicate and manage health data remotely. It covers different forms such as connected medical objects and devices.

- The expression "health professionals" covers all professionals recognised as such by national and European Union law practising in the health, medical welfare or social welfare sector, bound by professional secrecy and involved in co-ordinating treatment for an individual to whom they provide health care.

- The expression "health data hosting" denotes the use of third-party agencies for the secure and time-bound ~~lasting~~ storage of health data on the Internet .

- The expression "anonymisation" denotes the process applied to health data so that the data subject can no longer be identified, either directly or indirectly. Anonymisation is irreversible.

- The expression "pseudonymisation" denotes a technique whereby data can be made non-identifying for as long as they are not associated with other elements stored separately which would make identification possible.

- The concepts of "exchange" and "sharing" of health data, which can be features of health data processing, are defined as follows:

(a) "Data exchange" is the communication of information to a clearly identified recipient or recipients by a known transmitting party.

(b) "Data sharing" enables data to be made available to several persons entitled to be made aware of such data according to the principles of the right of access, without these persons necessarily being known at the outset.

- The term "communication" refers to any processing operation and in particular the exchange or sharing of personal data enabling authorised persons to have access to personal data, regardless of the means or devices used.

Chapter II

The legal conditions for use of health data

4. Privacy by design

4.1 Anyone processing health data must comply with the following principles:

Comment [BMG56]: Please define "medical objects". The term is not widely used and known. What is the difference between medical objects and medical devices?

Comment [BMG57]: Align with definition in Art. 3 (f) of the EU Directive 2011/234/EC on the application of patients' rights in cross-border healthcare.

Comment [BMG58]: Lasting storage would contradict the principle that sensitive data should only be stored for a period not beyond what is necessary for the purposes for which they are processed (see 4.1.d).

Comment [BMG59]: Exceeds Recital 26 GDPR (anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable) and Section 3 (6) of the Federal Data Protection Act (BDSG) ("Rendering anonymous" means the modification of personal data so that the information concerning personal or material circumstances can no longer or only with a disproportionate amount of time, expense and labour be attributed to an identified or identifiable individual).

Comment [BMG60]: align with Art. 4 (5) GDPR

Comment [BMG61]: Are concepts of exchange and sharing of health data an element of processing (see comment on the provision on the purpose)?

Comment [BMG62]: A definition of "processing" would be helpful.

Comment [BMG63]: Art. 5 GDPR uses "shall". This applies to a) through e).

~~e.~~g. *The processing of data should be proportionate in relation to the legitimate purpose pursued and shall be carried out only on the basis of free, specific, informed and ~~unambiguous~~ explicit consent of the data subject or on other legitimate basis laid down by law.*

~~f.~~h. *Personal data must be processed lawfully and fairly. They must be collected for explicit, specified and legitimate purposes and must not be processed in a manner that is incompatible with these purposes; subsequent processing for scientific or historical research purposes or statistical purposes in the public interest is compatible with those purposes on condition that additional guarantees apply.*

~~g.~~i. *The data must be adequate, relevant and not excessive in view of the purposes for which they are processed; they must be accurate and, if necessary, updated.*

~~h.~~j. *The data must not be stored in a form allowing identification of the data subjects for a period ~~not~~ beyond what is necessary for the purposes for which they are processed.*

~~i.~~k. *Appropriate ~~security~~ technical and organisational measures must be established to prevent risks such as accidental or unauthorised access to personal data or the destruction, loss, use, modification or disclosure to unauthorised ~~third~~ parties of those data.*

~~j.~~l. *The rights of the person whose data are collected and processed must be respected, particularly their rights of access to the data, communication, rectification and objection.*

4.2 The processing of health data is permissible only insofar as specific and appropriate guarantees are provided for in domestic law to prevent any risk to the interests, rights and fundamental freedoms of the data subject which the processing may represent, in particular the risk of discrimination.

4.3 The purposes for which health data are processed must also be taken into account in order to ensure appropriate use of these data and to adapt the safeguards accordingly.

4.4 In principle, health data must be collected and processed by health professionals, agencies acting under the responsibility of health professionals or by the data subjects themselves. Data controllers and their processors who are not health professionals should only collect and process health data in accordance with the same rules of confidentiality and security measures that apply to health professionals.

4.5 These personal data protection principles must be taken into account and incorporated right from the design of information systems ~~collecting, using and exploiting~~processing ~~of~~ health data. Compliance with these principles must be regularly reviewed throughout the life cycle of the processing. The controller must assess the impact of the applications used in terms of data protection and respect for privacy.

4.6 The controller must take all appropriate measures to fulfil their obligations with regard to data protection and must be able to demonstrate in particular to the competent supervisory authority that the processing for which they are responsible is in line with those obligations.

5. Processing of health data

5.1 Health data must be processed fairly and lawfully and only for specified purposes.

5.2 Health data shall in principle be collected from the data subject. They may be collected from other sources only if in accordance with principles 5, 6, 7, 9 and 12 of this Recommendation and if this is necessary to achieve the purpose of the processing or if the data subject is not in a position to provide the data.

5.3 Health data may be processed and communicated:

Formatted: Left, Space Before: 0 pt, After: 10 pt, Line spacing: Multiple 1,15 li, Numbered + Level: 1 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0,63 cm + Indent at: 1,27 cm

Comment [BMG64]: In accordance with Art. 9 (1) GDPR

Comment [BMG65]: In accordance with the GDPR

Comment [BMG66]: This wording could be interpreted to mean that the data must initially be stored in a form allowing identification of the data subjects. Proposed revision: "The data must not be stored in a form allowing identification of the data subjects for a period beyond"…

Comment [BMG67]: According to Art. 5 (1) (f) GDPR: "technical and organisational".

Comment [BMG68]: It should also be protected against internal data leaks (e.g. within the hospital or health care network to unauthorised employees).

Comment [BMG69]: The list here is questionable. What is the point of listing certain rights separately when all are to be respected equally?

Comment [BMG70]: Or "safeguards" in accordance with the GDPR

Comment [BMG71]: This differs from Section 203 of the Criminal Code and possibly also from labour law.

Comment [BMG72]: Data exploitation tends to have a negative connotation. Better "evaluating" or "analysing" or simply "processing"

Comment [BMG73]: It should be clarified under which conditions it is possible to collect data from sources other than the data subject.

Comment [BMG74]: Is communicating not an element of processing (see comment above)?

g. *if provided for by law or if the processing is based on a contract concluded with a health professional stipulating appropriate safeguards:*

- *ix. for preventive medical purposes and for purposes of medical diagnoses, administration of care or treatment, or management of health services by health professionals and those of the social and medical welfare sector;*
- *x. for reasons of public interest in the public health field, such as for example protection against international health hazards or in order to ensure a high standard of quality and safety for medical treatment, health products and medical devices;*
- *xi. for reasons of public interest in the field of managing claims for social ~~welfare~~ protection and health insurance benefits and services;*
- *xii. for reasons of public health provided they are lawful, legitimate and compatible with the initial purpose of the data collection;*

h. *if the data subject has given his or her consent in accordance with principle 12 of this Recommendation, except in cases where domestic law provides that a ban on processing health data cannot be lifted solely by the data subject's consent;*

i. *insofar as it is authorised by law:*

- *xi. for purposes of safeguarding the vital interests of the data subject or of a person physically or legally incapable of expressing consent;*
- *xii. for reasons relating to the obligations of the controllers and to the exercise of their rights or those of the data subject regarding employment and social protection, in accordance with domestic legislation or any collective agreement complying with the said legislation and providing for appropriate safeguards;*
- *xiii. for reasons essential to the recognition, exercise or defence of a legal claim;*
- *xiv. for reasons relating to scientific research in the field of health and the medical welfare sector;*
- *xv. for processing for statistical, historical or scientific research purposes under the conditions defined by domestic law to guarantee protection of the data subject's legitimate interests and where the individual cannot be identified from the results.*

In all cases, suitable guarantees must be established to ensure in particular the security of data and respect for the rights of the individual. Any other guarantees may be provided for in domestic law with a view to safeguarding respect for rights and fundamental freedoms.

6. Data concerning embryos and foetuses

6.1 ~~Medical~~ Health data concerning embryos and foetuses, inter alia such as data resulting from a pre-implantation diagnosis, should be considered as personal data and enjoy protection comparable to the protection of the health data of a minor.

6.2 Unless otherwise provided for by domestic law, the holder of parental responsibilities may act as the person legally entitled to act in the capacity of data subject.

Formatted: Left, Space Before: 0 pt, After: 10 pt, Line spacing: Multiple 1,15 li, Numbered + Level: 1 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 0,63 cm + Indent at: 1,27 cm

Comment [BMG75]: Align with Art. 9 (2) (h) GDPR, especially "administration of care or treatment".

Comment [BMG76]: in accordance with the GDPR

Comment [BMG77]: Is this regulatory content distinct from ii? If so, does it differ from the GDPR?

Comment [BMG78]: Align with Art. 9 (2) (f) GDPR.

Comment [BMG79]: In accordance with the GDPR the science privilege is limited to scientific research (and not commercial market research)

Comment [BMG80]: social protection? In accordance with the GDPR

Comment [BMG81]: BMG and BMBF: This goes beyond Art. 89 (1) GDPR, where pseudonymisation is one option but not a mandatory prerequisite. Measures for anonymisation or pseudonymisation may be used as safeguards but are not mandatory in every case for the processing of data for privileged purposes. Nor can the Convention be interpreted in that way. This passage should therefore be deleted.

Comment [BMG82]: The term "medical data" is used with reference to embryos and foetuses. We suggest using the broader term "health data" here as well, as in our view it is more comprehensive and thus offers broader data protection for this group.

Comment [BMG83]: Differs from the ability to provide consent as defined in Art. 8 (1) GDPR. The child may provide consent from the age of 16.

7. Genetic data

7.1 Genetic data processed with a preventive aim, for diagnosis or for treatment of the data subject or a third person (genetic testing on a legally incapacitated person for the benefit of family members for example) or for scientific research should be used only for these purposes or to enable the data subject to take a free and informed decision on these matters.

~~7.2 Processing of genetic data for the purpose of a judicial procedure or a criminal investigation should be the subject of a specific law offering appropriate safeguards. The data should be used only to establish whether there is a genetic link in the context of the production of evidence, to prevent a real danger or to punish a specific criminal offence. In no case should they be used to determine other characteristics which may be linked genetically.~~

7.3 Any processing of genetic data other than in the cases provided for in paragraphs 7.1 ~~and 7.2~~ should be authorised by the law, particularly where carried out to avoid any serious prejudice to the health of the data subject or third parties. Genetic data may not be used for commercial exploitation in any circumstances. The processing of genetic data in order to predict illness may be authorised in the vital interest and subject to appropriate safeguards provided for by law.

7.4 The publication of genetic data which would identify the data subject, a consanguine or uterine relative of the data subject, a member of his/her social family or a person who has a direct link with his/her genetic line, should be prohibited.

8. Shared medical secrecy for purposes of providing and administering care

8.1 Everyone is entitled to protection of his or her health data. The person receiving care is entitled to respect for his or her privacy and the secrecy of the information concerning them in dealings with a professional operating in the health, medical welfare and social sector.

8.2 In the interests of greater co-ordination between professionals operating in the health and social and medical welfare sector, the domestic law of each member State should recognise a shared professional secrecy, between professionals who are themselves legally bound by such secrecy.

8.3 The exchange and sharing of health data between health professionals must be limited to the information strictly necessary for the co-ordination or continuity of care, prevention or medical welfare-related and social monitoring of the individual, with the respective actors only able to pass on or receive data lying strictly within the scope of their tasks.

8.4 The data subject must be informed beforehand of the nature of the health data collected and processed and of the health professionals participating in the care team and must be able to object at any time to the exchange and sharing of his or her health data.

9. Communication to authorised third parties

9.1 Health data must not be communicated, except in the conditions set out in this Recommendation.

9.2 They may be communicated to third parties where the latter are authorised by domestic law to have ad hoc and limited access to the data. These third parties may be judicial authorities, experts appointed by a court authority or members of staff of an administrative authority designated by an official text.

9.3 Medical officers of insurance companies and employers cannot be regarded as third parties authorised to have access to the health data of patients. Member States may maintain or adopt specific rules on the processing of genetic data in connection with the conclusion of insurance contracts or in working life.

Comment [BMG84]: What exactly is meant by "preventive" ? – if it is understood as being synonymous to "predictive" the relation to paragraph 7.3, last sentence, should be clarified. Given the fact that diagnosis and treatment are referred to in this paragraph the correct word appears to be "predictive"

Comment [WU85]: Which preventive aim, any?

Comment [BMG86]: According to German legislation genetic testing for the benefit of a 3rd person is only allowed under specific conditions. Therefore, we propose to add a reference to national legislation as the basis for such genetic testing.

Comment [BMG87]: We would be grateful for an explanation of the practical meaning of this passage.

Comment [BMG88]: The recommendation is supposed to deal with health data. Therefore, genetic data should only be covered by this text where they are health related. Bearing this in mind, paragraph 7.2 should be deleted as it does not refer to health related genetic data.

Comment [BMG89]: Reference should be deleted following the comment on paragraph 7.2.

Comment [BMG90]: The processing of genetic data in order to predict illness may be authorised in the vital interest and subject to appropriate safeguards provided for by law.

Comment [BMG91]: Please explain the difference between "consanguine relative", "uterine relative" and "a person who has direct link with his/her genetic line" and why those three categories are necessary. The terms "consanguine" and "uterine" are not very common and might lead to unnecessary questions. Why does consanguinity only refer to the male gender? Do matrilinear relatives not share the same blood (at least half of it)? And what does their use add to the broader concept of "direct link with his/her genetic line"? The latter seems to also cover "consanguine" (patrilinear) and "uterine" (matrilinear) links. If there are no compelling grounds for all three categories, simple and inclusive language should be used.

Comment [BMG92]: This exception should be made already in the scope, if possible; see Art. 2 (2)(d) GDPR.

Comment [BMG93]: According to German legislation, genetic data may be processed under very specific conditions in connection with the conclusion of insurance contracts or in working life.

10. Storage of health data

10.1 Health data should be stored only for the time necessary to achieve the purposes for which they were collected. Domestic law may provide for exact storage periods having regard to the nature of the health data storage medium.

10.2 Storage of health data for other purposes than those for which they were initially collected must be carried out in compliance with the principles of this Recommendation.

10.3 The data subject may personally request deletion of his/her data unless they have been irreversibly rendered anonymous or legitimate interests preclude this.

Comment [BMG94]: Whose legitimate interest? Please explain.

Chapter III

The rights of the ~~individual~~data subject

11. Right to information

11.1 Everyone must be informed of the collection and processing of their health data.

They must be informed of:

- *~~1.~~ the identity and contact details of the controller and of the processors where relevant,*
- *~~2.~~ the purpose for which the data are processed, and where appropriate of the relevant legal basis for it,*
- *~~3.~~ how long the data will be stored,*
- *~~4.~~ the recipients of the data, and planned data transfers to a third country,*
- *~~5.~~ the possibility of refusing the processing of their data, or of withdrawing their initial consent, and the implications of such withdrawal,*
- *~~6.~~ the possibility of their data being subsequently processed for a compatible purpose, in accordance with appropriate safeguards provided for by domestic law,*
- *~~7.~~ the specific techniques used for processing their health data,*
- *~~8.~~ the conditions and the means made available to them for exercising via the controller their rights of access, the right of rectification and deletion of their health data, and the possibility to object to the processing thereof.*

Comment [BMG95]: Goes beyond Art. 13 (1)(a) GDPR.

Formatted: Left, Space Before: 0 pt, After: 10 pt, Line spacing: Multiple 1,15 li, Bulleted + Level: 1 + Aligned at: 0,63 cm + Indent at: 1,27 cm

Comment [BMG96]: Art. 13(1)(e) GDPR makes categories of data recipients sufficient.

Comment [WU97]: In which cases are transfers to a third country taken into consideration?

Comment [BMG98]: Not found in the GDPR.

11.2 This information should be provided at the time of data collection or of the first communication, unless it proves impossible or requires disproportionate efforts. It must be appropriate and suited to the circumstances. In particular, where the data subject is physically or legally incapable of receiving the information, it may be given to the person legally representing him/her. If a legally incapacitated person is capable of understanding, he/she should be informed before his/her data are processed.

11.3 Information provided to the data subject may be restricted if such derogation is provided for by law and constitutes a necessary and proportionate measure in a democratic society:

- *to prevent a real danger or to punish a criminal offence,*
- *for public health and social security reasons,*
- *to protect the subject and the rights and freedoms of others.*

Formatted: Left, Space Before: 0 pt, After: 10 pt, Line spacing: Multiple 1,15 li, Bulleted + Level: 1 + Aligned at: 0,63 cm + Indent at: 1,27 cm

Comment [WU99]: Which cases are meant?

Comment [BMG100]: In accordance with Art. 23 (1) (e) of the GDPR

Comment [WU101]: Which cases are meant?

11.4 ~~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. In a medical emergency, when the person's life is at stake, care takes precedence over information.~~

11.5 Domestic law must provide for appropriate safeguards ensuring respect for these rights.

12. Consent

12.1 Where the data subject is required to give his/her consent to the processing of health data, this consent should be free, specific, informed and explicit. When the consent is given digitally, it should be tracked. It does not absolve the person receiving it of the obligations to give prior information.

12.2 ~~The results of genetic analyses should be formulated within the limits of the objectives of the medical consultation, diagnosis or treatment for which consent was obtained.~~

12.3 Where it is intended to process health data relating to a legally incapacitated person who is incapable of free decision, and where domestic law does not authorise the data subject to act on his/her own behalf, consent is required from the person recognised as legally entitled to act in the interest of the data subject or from an authority or any person or body provided for by law.

12.4 If a legally incapacitated person has been informed of the intention to process his/her health data, his/her wishes should be taken into account, unless domestic law provides otherwise.

13. ***Right of access, objection and portability***

13.1 Everyone must be able to secure access to his or her health data directly from whoever holds them.

13.2 The right of access, implying the right to communication of information, on paper as well, enables the data subject to exercise his/her right of rectification and deletion. It also encompasses the right to receive data in a structured format making it possible to transmit them to another controller designated by the data subject.

13.3 The right of deletion is exercised subject to the cases prescribed by domestic law invoking legitimate grounds. The data subject is entitled to object on legitimate grounds to the collection of his/her personal health data except where the person holding the data invokes an overriding and legitimate reason concerning the public interest of public health.

13.4 If the request to rectify or delete the data is refused or if the data subject's objection is rejected, he or she must be able to appeal.

13.5 Access to health data may be refused, limited or delayed only if the law provides for it and if:

~~a.~~e. this constitutes a necessary and appropriate measure in a democratic society in the interests of protecting national security or public safety, or of preventing, investigating or punishing criminal offences; or

~~b.~~f. knowledge of the information is likely to cause serious harm to the data subject's health; or

~~c.~~g. ~~the information on the data subject also reveals information on third parties or if, with respect to genetic data, this information is likely to cause serious harm to a~~

Comment [BMG102]: Does this regulatory content extend beyond 11.2, first and second sentences? If so, please explain; if not, please delete.

Comment [BMG103]: Paragraph 11.4 has nothing to do with data protection rules and with the protection of genetic data. It is a direct interference into the doctor/patient relationship.
Paragraph 11.4 should be deleted.

Comment [WU104]: Compare the addition on "broad consent" in the research context in Chapter V.

Comment [WU105]: Digital consent should be formulatedAs to digital consent it should be guaranteed that,
1. the data subject has consciously and unambiguously given his consent,
2. a record of the consent is kept,
3. the data subject can access the content of the approval at any time, and
4. the data subject can revoke the consent at any time.

Comment [BMG106]: Paragraph 12.2 has nothing to do with data protection rules and with the protection of genetic data. It is a direct interference into the doctor/patient relationship.
Paragraph 12.2 should be deleted.

Comment [BMG107]: Must be revised in line with Art. 21 (1) GDPR. Firstly, the data subject is also entitled to object in the case of overriding contrary interests – but the objection will be unsuccessful. Secondly, according to Art. 21 (1) GDPR, no "legitimate grounds" are needed to object. All that is needed are "grounds relating to [the data subject's] particular situation". Further, "overriding and legitimate reasons" are not sufficient to reject the data subject's objection; instead, "compelling legitimate grounds" are required.

Comment [BMG108]: Where?

Formatted: Left, Space Before: 0 pt, After: 10 pt, Line spacing: Multiple 1,15 li, Numbered + Level: 1 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 1 cm + Indent at: 2,27 cm

Comment [BMG109]: Does that mean that a patient would not have access to his own health data because it may cause serious harm? How is serious harm defined? Who decides when serious harm is likely (government, health professional, the data subject)?
Paragraph 13.5 b) cannot be supported.

Comment [BMG110]: Is this how Article 23 (1)(i) GDPR is to be interpreted?

Comment [WU111]: Who decides whether the information is likely to cause serious harm to the data subject?

~~*consanguine or uterine relative or to a person who has a direct link with this genetic line;* or~~

~~*d.*~~ h. *the data are used for scientific or historical research purposes or statistical purposes where there is no identifiable risk of an infringement of the rights and fundamental freedoms of data subjects, in particular where such data are not used for decisions or measures relating to a specific individual.*

~~*13.6 The person subjected to genetic analysis should be informed of unexpected findings if the following conditions are met:*~~

~~*i. domestic law does not prohibit the provision of such information;*~~

~~*ii. the person himself or herself has asked for this information;*~~

~~*iii. the information is not likely to cause serious harm;*~~

~~*a. to his/her health; or*~~

~~*b. to a consanguine or uterine relative, to a member of his/her social family, or to a person who has a direct link with his/her genetic line, unless domestic law provides other appropriate safeguards:*~~

Subject to domestic law, the person should also be informed if this information is of direct importance to him/her for treatment or prevention.

Chapter IV

Reference frameworks for the processing of health data

In the processing of health data all players must observe high standards to ensure the confidentiality of particularly sensitive health data. The possible uses of these data and their disclosure, whether voluntary or not, are potentially highly damaging to an individual. But the issues of data availability (when a critical medical act is to be carried out, for example), integrity and auditability (including traceability) are equally vital.

As the use of digital technology leads to better care, technical considerations take on an ethical dimension, with data availability and interoperability converging with the notion of continuity of care and equality, and technical irreversibility potentially resulting in a loss of opportunity for patients for example.

14. Reference frameworks

14.1 In accordance with the principle of privacy by design as defined in paragraph 4.5, the applications which manage health data must, from their design onwards, incorporate the principles of data protection and the relevant security and interoperability reference frameworks and ensure that the processing of the data complies with these principles and reference frameworks.

14.2 The aim of these reference frameworks is, depending on the use made of data, to define in co-ordination with all the players the conditions governing the use of health data in information systems with a view to ensuring their confidentiality and interoperability. They cover the areas of identification, interoperability and security.

15. Interoperability reference frameworks

Comment [BMG112]: Does that mean that access to one's own genetic data may be denied in case of a possible harm to a 3rd person? Who defines what serious harm may be? For instance, could a person be denied access to the results of genetic analysis revealing that he will be confronted with Huntington's disease only because it means that his offspring will most likely also be affected?
Paragraph 13.5 c) cannot be supported.

Formatted: Left, Space Before: 0 pt, After: 10 pt, Line spacing: Multiple 1,15 li, Numbered + Level: 1 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 1,25 cm + Indent at: 2,52 cm

Comment [BMG113]: Please explain the difference between "consanguine relative", "uterine relative" and "a person who has direct link with his/her genetic line" and why those three categories are necessary. See 7.4

Comment [BMG114]: Paragraph 13.6 has nothing to do with data protection rules and with the protection of genetic data. It is a direct interference into the doctor/patient relationship and the right of the patient to take note or not to take note of the results of a genetic analysis concerning himself. Paragraph 13.6 should be deleted.

Comment [BMG115]: Please clarify which "reference frameworks" 14 refers to and who is to agree on them. They are apparently supposed to be agreed among the stakeholders (which ones?): 14.2 "The aim of these reference frameworks is, depending on the use made of data, to define in co-ordination with all the players the conditions governing the use of health data in information systems with a view to ensuring their confidentiality and interoperability." This requires further explanation. Only then can the provision be evaluated.

Comment [BMG116]: Please clarify which "interoperability reference frameworks" 15 refers to and who is to agree on them. This requires further explanation. Only then can the provision be evaluated.

15.1 These reference frameworks specify the standards to be used in the exchange or sharing of health data between information systems so that an IT component or system can work together with other existing or future components or systems. They entail using common language (semantic interoperability) and technical reference frameworks (technical interoperability).

15.2 To ensure respect for the rights of data subjects and to enable the development of efficient information systems, health professionals and patients together with any agency authorised to process personal health data, particularly the persons responsible for platforms which allow exchange and sharing of health data, must comply with the security rules and reference frameworks which may be given force of law under each country's domestic law, for example by using a certification process, to be accepted by all players. These rules and reference framework should be complied with particularly where health data are collected and processed in connection with care and treatment.

15.3 The aim of these reference frameworks is to define standards enabling health data to be exchanged and shared by information systems and to monitor their implementation under the conditions of security required.

15.4 They are based on the following principles.

- *g) using common language and formats of shared or exchanged content based on common standards (semantic interoperability);*
- *h) using interoperable services and common rules on use;*
- *i) using secure interconnection and information delivery protocols for data transport;*
- *j) guaranteeing data subjects reliable identification to ensure the uniqueness of their identity within the different information systems. The identifier chosen must be single, unequivocal, lasting and recognised by all operatives, and founded on a reliable certification system;*
- *k) ensuring authentication of the persons and systems involved in the processing of the data by means of arrangements which all operatives recognise and are such as to guarantee security in the exchange and sharing of the data;*
- *l) using secure solutions as defined in Principle 16.*

Formatted: Left, Space Before: 0 pt, After: 10 pt, Line spacing: Multiple 1,15 li, Numbered + Level: 1 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 1,5 cm + Indent at: 2,77 cm

16. Security reference frameworks

Comment [BMG117]: Please clarify which "security reference networks" 16 refers to and who is supposed to agree on them. This requires further explanation. Only then can the provision be evaluated.

16.1 The processing of health data must be secure and use solutions guaranteeing the availability, integrity, confidentiality and auditability of data.

16.2 These security rules, kept constantly state-of-the-art, should result in the adoption of such technical and organisational measures as to protect personal health data from any illegal or accidental destruction, any loss or any impairment, and to guard against any unauthorised access. In particular, domestic law must make provision for organising and regulating health data collection, storage and restitution procedures.

16.3 System availability– i.e. the proper functioning of the system – must be ensured by measures enabling the data to be made accessible in a secure way and with due regard for each person's permissions.

16.4 Guaranteeing integrity requires verification of every action carried out on the nature of the data, any changes made to or deletion of data, including the communication of data.

16.5 Data confidentiality requires the establishment of measures to monitor access to the data servers and the data themselves, ensuring that only authorised persons are able to access the data.

16.6 Auditability means that there must be a system making it possible to trace any access to the information system and for any action carried out by an individual to be logged to that individual.

16.7 Activity entailing storing health data on the Internet and making them available for users must comply with the security reference framework and principles of personal data protection.

16.8 Professionals who are not directly involved in the person's health care, but by virtue of their assigned tasks ensure the smooth operation of the information systems, may have access, insofar as this is necessary for the fulfilment of their duties and on an ad hoc basis, to personal health data. They must have full regard for professional secrecy and with appropriate measures laid down in domestic law to guarantee the confidentiality and security of the data.

17. Health data management services

17.1 Each member state should establish services for the exchange and sharing of health data as useful aids especially for the co-ordination of care, complying with security and interoperability reference framework defined in sections 14 to 16.

Since these capabilities for exchange and sharing contribute to the quality of care provision and to the proper management of health systems as well as to other goals, for the benefit of both individuals and the collective interest and public health, professionals in the health and social and medical welfare sector should each be equipped for the electronic management of their activity, enabling them to exchange or share personal health data.

17.2 ~~Patients must have the benefit of a secure electronic medical file enabling them to have information useful to their medical, welfare and social monitoring throughout their course of treatment~~.

The information in this medical file may be shared, with the patient's consent, by professionals involved in care provision for the patient in the conditions defined in paragraph 8.1.

17.3 Any electronic messaging system permitting the exchange of personal health data must comply with the reference framework defined in section 14.

Chapter V - Research in the health field

18. Research in the health field

18.1 The use of health data for the purposes of research in the health field ~~must~~ should be be carried out with a legitimate aim and in full compliance with the principles laid down in this Recommendation. and in accordance with recognised ethical standards for scientific research.

18.2 The need to use health data must be evaluated in the light of the aim pursued.

18.3 Persons whose data are being used for research must be informed of such use and, where provided for in domestic law, give their consent, except if no consent can be given in cases of medical emergency. If consent is requested data subjects should have the opportunity to give their consent to certain areas of scientific research to the extent allowed by the intended purpose.

When the data subject is a legally incapacitated person and domestic law does not authorise the data subject to act on his/her own behalf, his/her legal representative or an authority, or any person or body provided for by law, shall be provided with the information and/or shall give his or her consent in the context of the research project.

Comment [WU118]: What is meant by that?

Comment [BMG119]: We cannot agree with this until the question of reference networks has been clarified (see 14–16 above). Only then can this provision be evaluated.

Comment [BMG120]: Please clarify who is supposed to be responsible for equipping them.

Comment [BMG121]: This sounds as though it is supposed to provide grounds for a patient's claim to an electronic medical file. Germany does not yet have such electronic medical files. For this reason, we cannot support such a requirement.

Comment [BMG 2122]: These are recommendations.

Comment [WU123]: This wording is the same as in the GDPR and makes clear that, in addition to the data protection recommendations, also the generally recognised ethical standards for scientific research should be adhered to. Argument: consistency with the GDPR.

Comment [BMG 2124]: Clarify that in emergency cases it may be impossible for consent to be given.

Comment [WU125]: Clarify that in emergency cases it may be impossible for consent to be given.

Comment [BMG126]: This point needs to be thoroughly examined in order to identify potential conflicts with the provisions in the GDPR. For legal clarity, we suggest aligning it to the GDPR provisions.

Comment [WU127]: Because the actor here is the researcher, this wording seems more effective (in line with Recital 33, third sentence GDPR).

Comment [BD/128]: BMBF: Clarify that "broad consent" is permitted in the research context. In our view, such a reference is needed for a consistent interpretation of the GDPR and Convention (Recital 33 GDPR).
Der broad consent wurde auch in die neu überarbeitete Empfehlung zur Forschung mit humanbiologischem Material CM/(Rec(2016)6 aufgenommen, s. dort Artikel 19. Die Empfehlung gilt auch für die mit dem humanbiologischen Material verbundenen Daten.

Comment [BMG 2129]: In line with Recital 33, third sentence GDPR.

Comment [WU130]: In line with Recital 33, third sentence GDPR.

18.4 The conditions in which health data are processed for research in the health field ~~and, in particular, the value of such data for public health~~ must be assessed by the body or bodies designated by domestic law;

18.5 ~~Subject to additional provisions determined by domestic law,~~ ~~health~~Health-care professionals entitled to carry out their own medical research as well as scientists from other disciplines should be able to use the health data which they hold as long as the data subject has been informed of this possibility and ~~has not objected~~ has consented.

18.6 Personal data used for scientific research may not be published in a form which enables the data subjects to be identified, unless they have given their consent for the publication and publication is authorised by domestic law.

In all cases appropriate safeguards must be introduced to ensure in particular data security and respect for the rights of the individual. ~~-~~Any other guarantees may be provided for in domestic law with a view to safeguarding respect for rights and fundamental freedoms.

Chapter VI – Mobile applications

19. Mobile applications

19.1 The development of mobile applications enables both patients and professionals in the health sector and the welfare and social sector to collect health data and process them remotely. This development takes on different forms and covers several categories of applications, themselves pursuing very different goals of use. Ranging from medical applications to "quantified self" applications, connected devices make it possible to quantify and/or evaluate parameters that may reveal a person's state of health and, in certain cases, are used directly to make diagnoses and provide care.

19.2 Where the data collected by these applications may reveal a person's state of health, concern any information regarding their health care and welfare provision and/or are processed in a medical context, they constitute health data. In this connection they must enjoy the same legal protection and confidentiality applicable to other methods of health data processing as defined by the present Recommendation and, where applicable, supplemented by the domestic law of States.

19.3 Well-being or self-measurement applications used solely for the benefit of the individual using them, operated for solely personal reasons and not generating any external communication, data collection or transfer should not be considered as being subject to the requirements of the present Recommendation. Guidance on the application of data protection principles to the processing of health data by private sector entities in the context of the use of mobile applications is to be provided distinctly from the present Recommendation.

Comment [WU131]: It is first necessary to clarify what the authors mean by "research in the health field". Are they talking about any kind of research using health data or about research using medical data in the health-care sector?

To do so, it would also be important to clarify whether the recommendations are intended to refer to the protection of health data in general (title, purpose, scope) or specifically to protection for data processing in the health-care sector (3rd indent of the recommendations on p. 3, focus on the health-care sector in no. 18.4 and restriction to health-care professionals in no. 18.5).

Comment [WU132]: This scope is too narrow for research. It concerns not only research in the health-care sector. Without the deletion, it would not sufficiently cover medical research ranging from basic research to applied research!

Comment [WU133]: Restricting this to "health-care professionals" is too narrow. Not only physicians work in medical research; human geneticists without a medical degree, biologists and others also work in the field of medical research. Th ...

Comment [WU134]: In our view, it is urgently necessary to examine this point for compliance with the GDPR. It could result in every scientist engaged in medical research being allowed to process personal health data stored at hospitals or anywhe ...

Comment [BMG135]: This point also needs to be thoroughly examined in order to identify potential conflicts with the provisions in the GDPR. For legal clarity, we suggest aligning it to the GDPR provisions.

Comment [WU136]: Also with regard to health-care professionals entitled to carry out their own medical research there should be terms of deletion.

Comment [BMG137]: Why is this definition different from the one in I.3?

Comment [BMG138]: Unclear – the data protection provisions apply regardless of the technical application used.

Comment [BMG139]: What constitutes "external communication" (definition)? Does the transfer of data to the processor (app provider) also constitute external communication?

Comment [BMG140]: It is not entirely clear how extensive this exception from the scope of the recommendations is for apps for personal use. Does this sentence exempt personal apps (fitness armbands, blood pressure apps) for personal use from the ...

Comment [BMG141]: Is the regulatory content supposed to go beyond I.2. (3) (Limitation of scope with regard to "personal and household activity")? If so, this provision contradicts the GDPR and should be deleted. ...

ITALY/ ITALIE

Recommendation CM/Rec(2016)…. of the Committee of Ministers to member States on the protection of health data
(adopted by the Committee of Ministers … 2016,
at the … meeting of the Ministers' Deputies)

States face major challenges today, relating to the processing of health data, which now takes place in an environment that has changed considerably since the adoption of Recommendation No. R (97)5 on the protection of medical data.

This changed environment is due to the phenomenon of data digitisation, made possible by the computerisation of the health sector and to the proliferation of exchanges of information arising from the development of the Internet.

Noteworthy features of this new environment are the growing computerisation of the professional sector and particularly of activities relating to health care and prevention, to life sciences research and to health system management, and also the increasing involvement of patients.

Comment [AP142]: Involvement in what? Health treatment?

Besides, mobility and the development of connected medical objects and devices contribute to new uses and to the production of a rapidly growing volume of data.

Against this background, ~~This assessment shared by the member States has prompted to propose~~ a revision of Recommendation No. R (97) 5 on the protection of medical data has been considered necessary in order to respond to the numerous challenges for the right to private life and the protection of personal data raised by new technologies. In this context, the reference to ~~, with~~ the more general term "health data" (rather than "medical data") is ~~being~~ preferred, as it better mirrors the wide range of data processing related to health which may have a considerable impact on individual's private sphere.

Health data is indeed one of the special categories of data which - according to Article 6 of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108 – "Convention 108/1981") – deserves a strengthened protection because of the risk of discrimination deriving from improper processing. ~~while reaffirming the sensitivity of health data and the importance of regulating their use so as to guarantee due regard for the rights and fundamental freedoms of the individual, in particular the right to privacy~~.

Comment [AP143]: The legal background of this Recommendation in particular Convention 108 and the special protection granted to health data by Article 6, should be explicitly mentioned.

The Committee of Ministers, under the terms of Article 15.b of the Statute of the Council of Europe, recommends that the member States:

- ensure that the principles set forth in the appendix to the present Recommendation, which replaces Recommendation No. R (97) 5 mentioned above, are reflected in the implementation of national legislation on protection of health data, as well as in other branches of any law on the use of health data;

- ensure, to that end, that the present Recommendation and its appendix are brought to the attention of the authorities set up under national data protection legislation to monitor the application of that legislation, as well as of the authorities responsible for healthcare systems;

- promote acceptance and application of the principles set forth in the appendix to the present Recommendation, using additional instruments such as codes of conduct, while ensuring that these principles are well-known, understood and applied by all the players in the healthcare sector and taken into account in the design, deployment and use of the ICTs in that sector.

Appendix to Recommendation CM/Rec(2016)…

Chapter I
General provisions

Purpose

The purpose of this Recommendation is to provide member States with guidance for regulating the processing, and the different uses, of health data in order to guarantee respect for the rights and fundamental freedoms of every natural person, particularly the right to ~~privacy~~private life and to the protection of personal data as provided for by Article 8 of the European Convention on Human Rights and Convention 108/1981. ~~It also provides guidelines for developing interoperable and secured information systems in a manner enabling the quality of care and the efficiency of health systems to be enhanced.~~

Scope

This Recommendation is applicable to the processing of personal data relating to health (health data) in the public and private sectors.

It also lays down the principles for the exchange and sharing of health data by means of digital tools with due regard for the rights of the individual and the confidentiality of data.

The provisions of this Recommendation do not apply to health data processing performed by individuals in the context of ~~exclusively~~ purely personal or ~~domestic~~ household activities.

Definitions

For the purposes of this Recommendation, the following expressions are defined as follows:

- The expression “personal data” refers to any information relating to an identified or identifiable individual. An individual shall not be regarded as “identifiable” if identification requires an unreasonable amount of time and effort. In cases where the individual is not identifiable, the data are referred to as anonymous.

- The expression “health data” covers all data that may reveal the data subject’s past, present or future state of health in relation to his/her physical and/or mental condition, irrespective of their source. It also covers any information relating to his/her health, including the provisions of health care services which reveal information about her health status ~~and welfare provision~~. It may also involve information of a biological and genetic nature. It further covers data relating to well-being and/or lifestyle where these reveal a state of health.

- The expression “genetic data” refers to any data relating to an individual's genetic characteristics, whether inherited or acquired at an early stage of prenatal development, in particular resulting from the analysis of a biological sample from that individual: analysis of chromosomes, DNA or RNA or any other component making it possible to obtain equivalent information.

- The expression "reference framework" denotes a coordinated set of rules and/or processes kept constantly state-of-the-art and applicable to health information systems, covering the areas of identification, interoperability and security.

- The expression "electronic medical file" denotes a secured set of health data, structured or not, on electronic form, ~~of~~ related to one individual, ~~which accompanies them~~ throughout the course of their treatment. It enables the patient and authorised health professionals to share the information that is useful for co-ordinating care.

- The expression "secure messaging system" denotes a service for the secure exchange of personal health data between ~~identified~~ authorised? individuals.

- The expression "right to portability" denotes a person's right to receive data concerning them that have been ~~entrusted~~ provided to a data controller, in a structured, commonly used format, and to transmit them, if necessary, to another controller.

Comment [AP144]: We are not sure this should be the aim of a data protection recommendation. Maybe we can simply say that appropriate processing compliant with data protection principles can substantially contribute to the quality of health care and efficiency of health systems

Comment [AP145]: Sharing between whom? Health professionals?

Comment [AP146]: The suggested wording is line with the modernised Convention

Comment [AP147]: Not clear. Provision of social care services?

Comment [AP148]: Do genetic data necessarily result from the analysis of a biological sample? Should we add “in particular”?

Comment [AP149]: Not sure that this definition is clear enough

- The expression "mobile applications" denotes a set of means accessible in a mobile environment making it possible to communicate and manage health data remotely. It covers different forms such as connected medical objects and devices.

- The expression “health professionals” covers all professionals recognised as such by national and European Union law practising in the health, medical welfare or social welfare sector, bound by professional secrecy and involved in co-ordinating treatment for an individual to whom they provide health care.

- The expression "health data hosting" denotes the use of third-party agencies for the secure and lasting storage of health data on the Internet.

- The expression "anonymisation" denotes the process applied to health data so that the data subject can no longer be identified, either directly or indirectly. Anonymisation is irreversible.

- The expression "pseudonymisation" denotes a technique whereby data can be made non-identifying for as long as they are not associated with other elements stored separately which would make identification possible.

- The concepts of exchange and sharing of health data, which can be features of health data processing, are defined as follows:

(a) Data exchange is the communication of information to a clearly identified recipient or recipients by a known transmitting party.

(b) Data sharing enables data to be made available to several persons entitled to be made aware of such data according to the principles of the right of access, without these persons necessarily being known at the outset.

- The term communication refers to any processing operation and in particular the exchange or sharing of personal data enabling authorised persons to have access to personal data, regardless of the means or devices used.

Comment [AP150]: We are not sure the definition is clear. Data exchange would require reciprocal communication between two or more subjects. What we see here is more the definition of “communication” which, contrarily to “dissemination”, is directed to an identified recipient.

Comment [AP151]: We should not use this expression as it may be confused with data subject’s right to access to personal data or with the right of access to official documents

Comment [AP152]: These definitions may create some confusion. Do we really need them?

Chapter II

~~**The legal conditions for use of health data**~~

4. ~~Privacy by design~~ Legitimacy of data processing and quality of data

4.1 Anyone processing health data must comply with the following principles:

~~e.~~a. The processing of data should be proportionate in relation to the legitimate purpose pursued and shall be carried out only on the basis of free, specific, informed and ~~unambiguous~~ explicit consent of the data subject or on other legitimate basis laid down by law.

Comment [AP153]: See para 55 of the Explanatory Report of the modernised Convention

~~f.~~b. Personal data must be processed lawfully and fairly. They must be collected for explicit, specified and legitimate purposes and must not be processed in a manner that is incompatible with these purposes; subsequent processing for scientific or historical research purposes or statistical purposes is compatible with those purposes on condition that additional guarantees apply.

~~g.~~c. The data must be adequate, relevant and not excessive in view of the purposes for which they are processed; they must be accurate and, if necessary, updated.

~~h.~~d. The data must be stored in a form allowing identification of the data subjects for a period not beyond what is necessary for the purposes for which they are processed.

Appropriate security measures taking into account the technical state of the art and of the sensitive

Comment [AP154]: This is true for any kind of personal data. Can we emphasize the fact that health data needs more stringent protection as it was in the original text of the Recommendation?

nature of health data and the evaluation of potential risks, must be established to prevent risks such as accidental or unauthorised access to personal data or the destruction, loss, use, modification or disclosure to unauthorised third parties of those data.

e. The rights of the person whose data are collected and processed must be respected, particularly their rights of access to the data, communication, rectification and objection.

4.2 The processing of health data is permissible only insofar as specific and appropriate guarantees are provided for in domestic law to prevent any risk to the interests, rights and fundamental freedoms of the data subject which the processing may represent, in particular the risk of discrimination.

4.3 The purposes for which health data are processed must also be taken into account in order to ensure appropriate use of these data and to adapt the safeguards accordingly.

Comment [AP155]: Is this necessary? See 4.1

4.4 In principle, health data must be collected and processed by health professionals, agencies acting under the responsibility of health professionals or by the data subjects themselves. Data controllers and their processors who are not health professionals should only collect and process health data in accordance with the same rules of confidentiality and security measures that apply to health professionals.

4.bis Additional obligations

~~5.~~ 1 These personal data protection principles must be taken into account and incorporated right from the design of information systems collecting, using and exploiting health data. Compliance with these principles must be regularly reviewed throughout the life cycle of the processing. The controller must assess the impact of the applications used in terms of data protection and respect for privacy.

~~4.6~~2 The controller must take all appropriate measures to fulfil their obligations with regard to data protection and must be able to demonstrate in particular to the competent supervisory authority that the processing for which they are responsible is in line with those obligations.

Comment [AP156]: These two paragraphs refer to privacy by design, risk assessment and accountability which would deserve to be considered on a separate article under "additional obligations" (as in the modernised Convention)

5. Processing of health data

5.1 Health data must be processed fairly and lawfully and only for specified purposes.

Comment [AP157]: It is already in Article 4

5.2 Health data shall in principle be collected from the data subject. They may be collected from other sources only if in accordance with principles 5, 6, 7, 9 and 12 of this Recommendation and if this is necessary to achieve the purpose of the processing or if the data subject is not in a position to provide the data.

5.3 Health data may be processed ~~and communicated~~:

a. if provided for by law or if the processing is based on a contract concluded with a health professional stipulating appropriate safeguards:

~~iv.~~i. for preventive medical purposes and for purposes of medical diagnoses, administration of care or treatment, or management of health services by health professionals or provision of social care or treatment or management of social care systems ~~and by those of the~~ social ~~and~~ care professionals~~medical welfare services sector~~;

~~v.~~ii. for reasons of public interest in the public health field, such as for example protection against international health ~~hazards~~ threats or in order to ensure a high standard of quality and safety for medical treatment, ~~health~~ medicinal products and medical devices;

~~vi.~~iii. for reasons of public interest in the field of managing claims for social and health care services~~welfare and health insurance benefits and services~~;

~~vii.~~iv. for reasons of public health provided they are lawful, legitimate and compatible with the initial purpose of the data collection;

Comment [AP158]: What is the relationship between 5.3 a.i and 5.3.a.ii.?

Comment [AP159]: See previous comment

b. if the data subject has given his or her consent in accordance with principle 12 of this Recommendation, except in cases where domestic law provides that a ban on processing

health data cannot be lifted solely by the data subject's consent;

c. insofar as it is authorised by law:
   i. for purposes of safeguarding the vital interests of the data subject or of a ~~person physically or legally incapable of expressing consent~~third person;
   ii; for reasons relating to the obligations of the controllers and to the exercise of their rights or those of the data subject regarding employment and social protection, in accordance with domestic legislation or any collective agreement complying with the said legislation and providing for appropriate safeguards;
   iii. for reasons essential to the recognition, exercise or defence of a legal claim;
   iv. for reasons relating to research in the field of health and the medical welfare sector;
   v. for processing for statistical, historical or scientific research purposes under the conditions defined by domestic law to guarantee protection of the data subject's legitimate interests and where the individual cannot be identified from the results.

In all cases, additional and suitable guarantees must be established to ensure in particular the security of data and respect for the rights of the individual. Any other guarantees may be provided for in domestic law with a view to safeguarding respect for rights and fundamental freedoms.

6. Data concerning embryos and foetuses

6.1 Medical data concerning embryos and foetuses, *inter alia* such as data resulting from a pre-implantation diagnosis, should be considered as personal data and enjoy protection comparable to the protection of the health data of a minor.

6.2 Unless otherwise provided for by domestic law, the holder of parental responsibilities may act as the person legally entitled to act in the capacity of data subject.

7. Genetic data

7.1 Genetic data processed with a preventive aim, for diagnosis or for treatment of the data subject or a third person ~~(genetic testing on a legally incapacitated person for the benefit of family members for example)~~ or for scientific research should be used only for these purposes or to enable the data subject to take a free and informed decision on these matters.

7.2 Processing of genetic data for the purpose of a judicial procedure or a criminal investigation should be the subject of a specific law offering appropriate safeguards. The data should be used only to establish whether there is a genetic link in the context of the production of evidence, to prevent a real danger or to punish a specific criminal offence. In no case should they be used to determine other characteristics which may be linked genetically.

7.3 Any processing of genetic data other than in the cases provided for in paragraphs 7.1 and 7.2 should be authorised by the law, for health reasons particularly where carried out to avoid any serious prejudice to the health of the data subject or third parties. Genetic data may not be used for commercial exploitation in any circumstances. The processing of genetic data in order to predict illness may be ~~authorised~~ carried out in the vital interest of the data subject or a third party and subject to appropriate safeguards provided for by law.

7.4 The publication of genetic data which would identify the data subject, a consanguine or uterine relative of the data subject, a member of his/her social family or a person who has a direct link with his/her genetic line, should be prohibited.

8. Shared medical secrecy for purposes of providing and administering care

8.1 Everyone is entitled to protection of his or her health data. The person receiving care is entitled to respect for his or her privacy and the secrecy of the information concerning them in dealings with a professional operating in the health, medical welfare and social sector.

Comment [AP160]: Not clear: "for reasons relating to the legal obligations to which the controller is bound?"

Comment [AP161]: As c.v refers to research as well, shouldn't we put iv and v together?

Comment [A162]: See par. 4.1.b

Comment [AP163]: The original recommendation referred to unborn children. Is there a specific reason to refer to embryos and foetuses?

Comment [AP164]: We should uniform the language (see Article 5.3)

Comment [AP165]: Is it too broad? Should we say a "grave and irreparable danger"?

Comment [AP166]: The reference to health reasons - which is in the original Recommendation - is relevant

Comment [AP167]: Isn't this already covered by 7.1?

Comment [AP168]: The "publication" should be prohibited in respect of any "health data" not only of genetic data

Comment [A169]: Not clear. Does it mean social care and social protection?

8.2 In the interests of greater co-ordination between professionals operating in the health and social and medical welfare sector, the domestic law of each member State should recognise a shared professional secrecy, between professionals who are themselves legally bound by such secrecy.

8.3 The exchange and sharing of data between health professionals must be limited to the information strictly necessary for the co-ordination or continuity of care, prevention or medical welfare-related and social monitoring of the individual, with the respective actors only able to pass on or receive data lying strictly within the scope of their tasks.

8.4 The data subject must be informed beforehand of the nature of the data collected and processed and of the health professionals participating in the care team and must be able to object at any time to the exchange and sharing of his or her health data.

Comment [A170]: Not clear. Does it mean social care and social protection?

Comment [A171]: Not clear. Does it mean "social care related services"?

Comment [AP172]: We would avoid this expression which sounds too broad and dangerously vague.

Comment [A173]: Does the data processing involve only medical professionals or other types of experts (such as professionals operating in the social care services)?

9. Communication to authorised third parties

9.1 Health data must not be communicated, except in the conditions set out in this Recommendation.

9.2 They may be communicated to third parties where the latter are authorised by domestic law to have ad hoc and limited access to the data. These third parties may be judicial authorities, experts appointed by a court authority or members of staff of an administrative authority designated by an official text.

9.3 Medical officers of insurance companies and employers cannot be regarded as third parties authorised to have access to the health data of patients.

Comment [AP174]: We would reword this sentence. Maybe "official authority"?

10. Storage of health data

10.1 Health data should be stored only for the time necessary to achieve the legitimate purposes for which they were collected. Domestic law may provide for exact storage periods having regard to the nature of the health data storage medium.

10.2 Storage of health data for other purposes than those for which they were initially collected must be carried out in compliance with the principles of this Recommendation.

10.3 The data subject may personally request deletion of his/her data unless they have been irreversibly rendered anonymous or legitimate interests overriding her/his interest preclude this.

Comment [AP175]: not clear what it refers to

Comment [AP176]: What does the word "personally" mean? Individually?

Chapter III

The rights of the individual

11. Right to information

11.1 Everyone must be informed of the collection and processing of their health data.

They must be informed of:

- the identity and contact details of the controller and of the processors where relevant,
- the purpose for which the data are processed, and where appropriate of the relevant legal basis for it,
- how long the data will be stored,
- the recipients of the data, and planned data transfers to a third country,
- the possibility of refusing the processing of their data, or of withdrawing their initial consent, and the implications of such withdrawal,
- the possibility of their data being subsequently processed for a compatible purpose, in accordance with appropriate safeguards provided for by domestic law,
- the specific techniques used for processing their health data,
- the conditions and the means made available to them for exercising via the controller their rights of access, the right of rectification and deletion of their health data, and the possibility to object to the processing thereof.

Comment [AP177]: ?

11.2 This information should be provided at the time of data collection or of the first communication, unless it proves impossible or requires disproportionate efforts. It must be appropriate and suited to the circumstances. In particular, where the data subject is physically or legally incapable of receiving the information, it may be given to the person legally representing him/her. If a legally incapacitated person is capable of understanding, he/she should be informed before his/her data are processed.

11.3 Information provided to the data subject may be restricted if such derogation is provided for by law and constitutes a necessary and proportionate measure in a democratic society:

- to prevent a real danger or to punish a criminal offence,
- for public health reasons,
- to protect the subject and the rights and freedoms of others.

Comment [A178]: Is it too broad? Should we say a "grave and irreparable danger"

11.4 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. In a medical emergency, when the person's life is at stake, care takes precedence over information.

11.5 Domestic law must provide for appropriate safeguards ensuring respect for these rights.

12. Consent

12.1 Where the data subject is required to give his/her consent to the processing of health data, this consent should be free, specific, informed and explicit. When the consent is given digitally, it should be tracked. It does not absolve the person receiving it of the obligations to give prior information.

12.2 The results of genetic analyses should be formulated within the limits of the objectives of the medical consultation, diagnosis or treatment for which consent was obtained.

12.3 Where it is intended to process health data relating to a legally incapacitated person who is incapable of free decision, and where domestic law does not authorise the data subject to act on his/her own behalf, consent is required from the person recognised as legally entitled to act in the interest of the data subject or from an authority or any person or body provided for by law.

12.4 If a legally incapacitated person has been informed of the intention to process his/her health data, his/her wishes should be taken into account, unless domestic law provides otherwise.

13. Right of access, objection and portability

13.1 Everyone must be able to secure access to his or her health data directly from whoever holds them.

13.2 The right of access, implying the right to communication of information, on paper as well, enables the data subject to exercise his/her right of rectification and deletion. It also encompasses the right to receive data in a structured format making it possible to transmit them to another controller designated by the data subject.

Comment [AP179]: It is true that the right to access enables the exercise of the right to rectification and deletion but it should be considered also as a stand-alone autonomous right.

13.3 The right of deletion is exercised subject to the cases prescribed by domestic law invoking legitimate grounds. The data subject is entitled to object on legitimate grounds to the collection of his/her personal health data except where the person holding the data invokes an overriding and legitimate reason concerning the public interest of public health.

Comment [AP180]: This is the right to portability which has a different function from the right to access.

13.4 If the request to rectify or delete the data is refused or if the data subject's objection is rejected, he or she must be able to appeal.

Comment [AP181]: For clarity sake it is advisable to refer to the right to erasure and the right to object in separate paragraphs

13.5 Access to health data may be refused, limited or delayed only if the law provides for it and if:

a. this constitutes a necessary and appropriate measure in a democratic society in the interests of protecting national security or public safety, or of preventing, investigating or punishing criminal offences; or

b. knowledge of the information is likely to cause serious harm to the data subject's health; or

c. the information on the data subject also reveals information on third parties or if, with respect to genetic data, this information is likely to cause serious harm to a consanguine or uterine relative or to a person who has a direct link with this genetic line; or

d. the data are used for scientific or historical research purposes or statistical purposes where there is no identifiable risk of an infringement of the rights and fundamental freedoms of data subjects, in particular where such data are not used for decisions or measures relating to a specific individual.

13.6 The person subjected to genetic analysis should be informed of unexpected findings if the following conditions are met:

a. domestic law does not prohibit the provision of such information;
b. the person himself or herself has asked for this information;
c. the information is not likely to cause serious harm;
   i. to his/her health; or
   ii. to a consanguine or uterine relative, to a member of his/her social family, or to a person who has a direct link with his/her genetic line, unless domestic law provides other appropriate safeguards;

Subject to domestic law, the person should also be informed if this information is of direct importance to him/her for treatment or prevention.

Comment [A182]: To exercise those rights, the person should be informed in advance of the possibility of expected findings otherwise

Comment [A183]: Isn't it too paternalistic?

Chapter IV

Reference frameworks for the processing of health data

In the processing of health data all players must observe high standards to ensure the confidentiality of particularly sensitive health data. The possible uses of these data and their disclosure, whether voluntary or not, are potentially highly damaging to an individual. But the issues of data availability (when a critical medical act is to be carried out, for example), integrity and auditability (including traceability) are equally vital.

As the use of digital technology leads to better care, technical considerations take on an ethical dimension, with data availability and interoperability converging with the notion of continuity of care and equality, and technical irreversibility potentially resulting in a loss of opportunity for patients for example.

Comment [AP184]: Not clear what the expression refers to

Comment [AP185]: The language of this chapter does not seem to be appropriate for a Recommendation

14. Reference frameworks

Comment [AP186]: We find the "reference frameworks" hard to understand

14.1 In accordance with the principle of privacy by design as defined in paragraph 4.5, the applications which manage health data must, from their design onwards, incorporate the principles of data protection and the relevant security and interoperability reference frameworks and ensure that the processing of the data complies with these principles and reference frameworks.

14.2 The aim of these reference frameworks is, depending on the use made of data, to define in co-ordination with all the players the conditions governing the use of health data in information systems with a view to ensuring their confidentiality and interoperability. They cover the areas of identification, interoperability and security.

15. Interoperability reference frameworks

Comment [AP187]: As stated before, I am not sure this section is a data protection issue. The perspective we should use here is eventually to ensure that also in interoperability data protection principles are fully complied with

15.1 These reference frameworks specify the standards to be used in the exchange or sharing of health data between information systems so that an IT component or system can work together with other existing or future components or systems. They entail using common language (semantic interoperability) and technical reference frameworks (technical interoperability).

15.2 To ensure respect for the rights of data subjects and to enable the development of efficient information systems, health professionals and patients together with any agency authorised to process personal health data, particularly the persons responsible for platforms which allow exchange and sharing of health data, must comply with the security rules and reference frameworks which may be given force of law under each country's domestic law, for example by using a certification process, to be accepted by all players. These rules and reference framework should be complied with particularly where health data are collected and processed in connection with care and treatment.

15.3 The aim of these reference frameworks is to define standards enabling health data to be exchanged and shared by information systems and to monitor their implementation under the conditions of security required.

15.4 They are based on the following principles.

a) using common language and formats of shared or exchanged content based on common standards (semantic interoperability);

b) using interoperable services and common rules on use;

c) using secure interconnection and information delivery protocols for data transport;

d) guaranteeing data subjects reliable identification to ensure the uniqueness of their identity within the different information systems. The identifier chosen must be single, unequivocal, lasting and recognised by all operatives, and founded on a reliable certification system;

e) ensuring authentication of the persons and systems involved in the processing of the data by means of arrangements which all operatives recognise and are such as to guarantee security in the exchange and sharing of the data;

f) using secure solutions as defined in Principle 16.

16. Security reference frameworks

16.1 The processing of health data must be secure and use solutions guaranteeing the availability, integrity, confidentiality and auditability of data.

16.2 These security rules, kept constantly state-of-the-art, should result in the adoption of such technical and organisational measures as to protect personal health data from any illegal or accidental destruction, any loss or any impairment, and to guard against any unauthorised access. In particular, domestic law must make provision for organising and regulating health data collection, storage and restitution procedures.

16.3 System availability– i.e. the proper functioning of the system – must be ensured by measures enabling the data to be made accessible in a secure way and with due regard for each person's permissions.

16.4 Guaranteeing integrity requires verification of every action carried out on the nature of the data, any changes made to or deletion of data, including the communication of data.

16.5 Data confidentiality requires the establishment of measures to monitor access to the data servers and the data themselves, ensuring that only authorised persons are able to access the data.

16.6 Auditability means that there must be a system making it possible to trace any access to the information system and for any action carried out by an individual to be logged to that individual.

16.7 Activity entailing storing health data on the Internet and making them available for users must comply with the security reference framework and principles of personal data protection.

16.8 Professionals who are not directly involved in the person's health care, but by virtue of their assigned tasks ensure the smooth operation of the information systems, may have access, insofar as this is necessary for the fulfilment of their duties and on an ad hoc basis, to personal health data. They must have full regard for professional secrecy and with appropriate measures laid down in domestic law to guarantee the confidentiality and security of the data.

17. Health data management services

17.1 Each member state should establish services for the exchange and sharing of health data as useful aids especially for the co-ordination of care, complying with security and interoperability reference framework defined in sections 14 to 16.

Comment [A188]: Not sure it is clear and related to data protection issues

Since these capabilities for exchange and sharing contribute to the quality of care provision and to the proper management of health systems as well as to other goals, for the benefit of both individuals and the collective interest and public health, professionals in the health and social and medical welfare

sector should each be equipped for the electronic management of their activity, enabling them to exchange or share personal health data.

17.2 Patients must have the benefit of a secure electronic medical file enabling them to have information useful to their medical, welfare and social monitoring throughout their course of treatment.

The information in this medical file may be shared, with the patient's consent, by professionals involved in care provision for the patient in the conditions defined in paragraph 8.1.

17.3 Any electronic messaging system permitting the exchange of personal health data must comply with the reference framework defined in section 14.

Comment [A189]: Not clear what the expression refers to.

Chapter V
Research in the health field

18. Research in the health field

18.1 The use of health data for the purposes of research in the health field must be carried out with a legitimate aim and in full compliance with the principles laid down in this Recommendation.

18.2 The need to use health data must be evaluated in the light of the aim pursued.

18.3 Persons whose data are being used for research must be informed of such use and, where provided for in domestic law, give their consent, except in cases of medical emergency.

When the data subject is a legally incapacitated person and domestic law does not authorise the data subject to act on his/her own behalf, his/her legal representative or an authority, or any person or body provided for by law, shall be provided with the information and/or shall give his or her consent in the context of the research project.

18.4 The conditions in which health data are processed for research in the health field and, in particular, the value of such data for public health must be assessed by the body or bodies designated by domestic law;

18.5 Subject to additional provisions determined by domestic law, health-care professionals entitled to carry out their own medical research should be able to use the health data which they hold as long as the data subject has been informed of this possibility and has not objected.

Comment [A190]: This paragraph (which was in the original recommendation) refers to opt out. Is this in line with para. 4.1?

18.6 Personal data used for scientific research may not be published in a form which enables the data subjects to be identified, unless they have given their consent for the publication and publication is authorised by domestic law.

In all cases appropriate safeguards must be introduced to ensure in particular data security and respect for the rights of the individual. Any other guarantees may be provided for in domestic law with a view to safeguarding respect for rights and fundamental freedoms.

Chapter VI

Mobile applications

19. Mobile applications

19.1 The development of mobile applications enables both patients and professionals in the health sector and the welfare and social sector to collect health data and process them remotely. This development takes on different forms and covers several categories of applications, themselves pursuing very different goals of use. Ranging from medical applications to "quantified self" applications, connected devices make it possible to quantify and/or evaluate parameters that may reveal a person's state of health and, in certain cases, are used directly to make diagnoses and provide care.

19.2 Where the data collected by these applications may reveal a person's state of health, concern any information regarding their health care and provisions of social care? ~~welfare provision~~ and/or are processed in a medical context, they constitute health data. In this connection they must enjoy the same legal protection and confidentiality applicable to other methods of health data processing as defined by the present Recommendation and, where applicable, supplemented by the domestic law of States.

19.3 Well-being or self-measurement applications used solely for the benefit of the individual using them, operated for solely personal reasons and not generating any external communication should not be considered as being subject to the requirements of the present Recommendation. Guidance on the application of data protection principles to the processing of health data by private sector entities in the context of the use of mobile applications is to be provided distinctly from the present Recommendation.

* * *

NORWAY / NORVEGE

TP-D – Norway's comments to the draft recommendation on health data

General remarks

Norway supports a revision/update of Recommendation No. R (97) 5. It is important that legal instruments (both binding and non-binding) regarding processing of personal health data are being kept up to date to reflect the technical developments in the health sector.

Norway's general position is that natural persons have a right to control their own personal data. Health data is a special category of personal data (sensitive data) which must enjoy heightened protection. In Norway's view, this should be a guiding principle throughout the recommendation.

Legal instruments on personal health data must reflect the need for strong data protection. At the same time, they must reflect the need for quality and efficiency of health systems, which benefits both individuals and society as a whole. In particular, Norway believes it is important to find the right balance between protecting the individuals' right to protection of their health data and the possibility of register-based research in the health field. Norway supports the comments from Sweden and Denmark in that respect.

Norway has the following specific remarks to the draft:

Section 1

The European Commission and Italy have suggested that the sentence "It also provides guidelines for developing interoperable and secured information systems in a manner enabling the quality of care and the efficiency of health systems to be enhanced", should be deleted.

In Norway's opinion, this sentence should remain. It is important that legal instruments on health data reflect both purposes.

Section 3

Norway believes the definition of "anonymisation", which includes the requirement that "anonymisation is irreversible", brings clarity to the concept of anonymisation. However, the definition could cause uncertainty as it seemingly sets a different – higher – threshold for anonymisation than in Convention 108 and the GDPR.

Norway supports the European Commission's written comments that it should be clarified in the definition of pseudonymised data that those are personal data.

Section 4

Norway agrees with Sweden that point 4.1 d should be supplemented so that storage of data for longer periods solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is allowed. This would be in line with article 5.1e of the General Data Protection Regulation and with the proposed modernised text of Convention 108.

Section 5

Norway supports Finland´s comment on point 5.3 ("for processing for statistical, historical or scientific research purposes under the conditions defined by domestic law to guarantee protection of the data subject's legitimate interests and where the individual cannot be identified from the results"). It is important to ensure that this will not preclude the use of the data later. Moreover, it is advisable to state that statistical or research purposes are not considered to conflict with the original purpose of use.

In point 5.3.c.iv, Norway supports the proposal from Germany to include the word "scientific" between "to" and "research".

Section 7

Norway recognises the privacy concerns connected with publication of genetic data. Norway however agrees with the European Commission that point 7.4 is worded in a way that is too absolute, since all genetic data in principle poses a risk of re-identification. In Norway's view, the recommendation should be worded in a way that emphasises the serious privacy concerns connected with publication of genetic data without taking the form of an absolute prohibition.

Section 8

Point 8.3 is too restrictive, in particular where health data are collected from sources other than the individual and processed in the public interest (e.g. for reasons of public health).

Point 8.4 states that the data subject must be informed *beforehand*. A requirement to individual information beforehand seems to be too restrictive, as there may be situations when health care is provided and there is no practical possibility to provide such information. In Norway, the patients in such situations may be provided general information for instance through the legislation.

Section 11

Point 11.1 requires that the data subjects must be informed of "the specific techniques used for processing their health data". As suggested by the European Commission, this is not a requirement under the GDPR and should be deleted.

Section 13

Point 13.5 b requires that access to health data may be refused, limited or delayed if "knowledge of the information is likely to cause serious harm to the data subject's health". Germany and the European Commission have suggested that this alternative should be deleted.

In Norway's opinion, this alternative should remain. We refer to the Norwegian Patients' Rights Act section 3-2 which states that "Information may be omitted if it is absolutely necessary in order to prevent endangering the patient's life or serious damage to the patient's health. Information may also be omitted if it is clearly inadvisable to provide such information out of consideration for persons who are close to the patient." The decision whether to omit information is taken by the health personnel responsible for the health care given to the patient.

Point 13.6 regulates information to the patient on unexpected findings after genetic analysis. Norway cannot see how these requirements constitute *data protection rules* and supports Germany's proposal to delete this point.

Section 15

Norway has concerns regarding section 15. The principal concern is also raised by Italy, and regards whether semantic interoperability needs to be part of these recommendations on privacy of health data. Semantic interoperability is an important but very difficult goal for health data, which will increase the quality and reusability of health data. However, whether data is structured or not does not mainly affect issues of privacy and data security. Data security needs to be put in place also for data that is not structured and not semantically interoperable. If privacy and data security is considered the central topic of this recommendation then Norway suggests taking these measures out.

If section 15 remains a part of the recommendations, Norway suggests loosening the description in the recommendation. Most of the health data used by health personnel today is not structured, and it will be very effortful to achieve the goals stated in the article, that all data should be structured and semantically interoperable.

SWEDEN/ SUEDE

Comments on the Draft Recommendation on the Protection of Health Data (version dated 9 May)

The Swedish position

Sweden's position is that since there are many remaining issues and questions concerning the Recommendation we cannot approve it at this point. Below Sweden has listed a number of changes in wording that would make it possible to approve the recommendation and would request that these are incorporated in the text. Sweden looks forward to further discuss the substance of the recommendation at the next meeting of the T-PD.

General comments

The protection of personal data is a fundamental right but it may, in certain circumstances such as the protection of health, be balanced in accordance with laws necessary in a democratic society. The processing of health data is important for various stakeholders such as patients, health care personal and scientists.

The Recommendation covers processing of personal data that are also regulated in the new EU Regulation 2016/679 General Data Protection Regulation. The work should continue in order to achieve that the Recommendation and the EU Regulation can coexist without problems for those who need processing health data.

Comments concerning specific articles

Sweden has some comments regarding to specific parts of the Recommendation which are presented below.

~~g.~~m. 3. Definitions

~~h.~~n. General comment to section 3

It is difficult to have definitions that differ from those in the General Data Protection Regulation (GDPR). The definition of 'genetic data' and 'pseudonymisation' needs to be the same as the Regulation.

~~i.~~o. Specific comments to section 3

- The expression "genetic data" refers to any data relating to an individual's genetic characteristics, whether inherited or acquired ~~at an early stage of prenatal development~~, resulting from the analysis of a biological sample from that individual: analysis of chromosomes, DNA or RNA or any other component making it possible to obtain equivalent information.

Motivation for changes above

It is often impossible to establish when a certain acquired genetic characteristic has appeared in an individual's life cycle. For example, acquired genetic characteristic that can result in malignant cancers can appear at any period during an individual's life cycle.

- The expression "pseudonymisation" denotes a technique and/or a organisational measure whereby data can be made non-identifying for as long as they are not associated with other elements stored separately which would make identification possible.

Motivation for changes above

According to GDPR:
'Pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

General comment
Data can be made non-identifying through organisational measures as well as technical measures or a combination of both measures.

~~j.~~p. 4. Privacy by design

The data must be stored in a form allowing identification of the data subjects for a period not beyond what is necessary for the purposes for which they are processed. Data may be stored for longer periods of time for statistical, historical or scientific research purposes under the conditions defined by domestic law.

Motivation for changes above
This article should be supplemented so that storage of data for longer periods for archival purposes or for the purpose of scientific or historical research is allowed, as long as appropriate technical and organisational measures are implemented to safeguard the rights and freedoms of the data subject. This would be in line with article 5.1e of the General Data Protection Regulation.

~~k.~~g. 5. Processing of health data

c. insofar as it is authorised by law:
   i. for purposes of safeguarding the vital interests of the data subject or of a person physically or legally incapable of expressing consent;
   ii. for reasons relating to the obligations of the controllers and third parties and to the exercise of their rights or those of the data subject regarding employment and social protection, in accordance with domestic legislation or any collective agreement complying with the said legislation and providing for appropriate safeguards;

Motivation for changes above
We have difficulties to fully understand 5.c.ii as the subsection is formulated in a complicated way. But as far as we can understand, the subsection leaves less room for third parties' processing than subsection 4.3.b.iii does in the current recommendation (Rec(97)5 13/02/1997 on the protection of medical data). Therefor we suggest that third parties 'processing, e.g. trade unions, is explicitly mentioned in the subsection.

iv. for reasons relating to research in the field of health and the medical welfare sector;
v. for processing for statistical, historical or scientific research purposes under the conditions defined by domestic law to guarantee protection of the data subject's legitimate interests and ~~where~~ provided that data relating to identified or identifiable ~~the~~ individuals cannot be identified ~~from~~ in ~~the~~ published results.

Motivation for changes above
These two parts should be adjusted to match articles 9.2 of the GDPR. All points in C may need to be analysed but especially these two. The purpose of 5.3(v) needs to be clarified.
General comment on section 5.3
How does section 5.3 relate to Recommendation CM/Rec(2015)5 on the processing of personal data in the context of employment, and specifically section 9.3–9.7? We notice that there are differences in formulations but we have difficulties to fully assess the implications of these differences.

l.r. 6. Data concerning embryos and foetuses

Compared to the draft from February, SE notes some changes of the wording of article 6. In front of the further preparation of the draft, SE would like to get some information about the causes of these changes.

m.s. 7. Genetic data

7.1 Genetic data processed with a preventive aim, for diagnosis or for treatment of the data subject or a third person (genetic testing on a legally incapacitated person for the benefit of family members for example) or for scientific research should be used only for these purposes or other compatible purposes or to enable the data subject to take a free and informed decision on these matters.

Motivation for changes above

It is important that there is the possibility to use genetic data from analysis of biological material from identifiable persons in health care for research. Such information may only be used under certain circumstances and with certain safeguards (consent, ethics reviews, etc.)

---

n.t. Section 7.4

This section should be deleted.

Motivation for changes above

This article should be deleted. Legislation on when information can or cannot be published varies between countries. In many countries, e.g. Sweden, these questions are regulated in the constitution and in ethical guidelines. Therefore we believe that it is not appropriate to regulate this issue in the Recommendation.

o.u. Section 9

This article is problematic since the scope becomes too narrow or constricted. There must a possibility to communicate medical data in more situations. Compare with article 9 in General Data Protection Regulation.

p.v. 10. Storage of health data

10.1 Health data should be stored only for the time necessary to achieve the purposes for which they were collected. However, data may be stored for longer periods of time for statistical, historical or scientific research purposes under the conditions defined by domestic law. Domestic law may provide for exact storage periods having regard to the nature of the health data storage medium.

Motivation for changes above

GDPR:

Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject.

10.3 The data subject may personally request deletion of his/her data unless they have been irreversibly rendered anonymous or legitimate interests or domestic law preclude this.

Motivation for changes above

This right should primarily concern data that has been collected with consent. The recommendation must allow for health registers regulated by national law. One cannot have the right to be erased from such health data registers. This part in the recommendation should also be adapted to how article 17 in the GDPR is written, see art. 17.3(d).

q.w. 11. Right to information

11.1 Everyone must be informed of the collection and processing of their health data.

They must be informed of:

- the identity and contact details of the controller and of the processors where relevant,
- the purpose for which the data are processed, and where appropriate of the relevant legal basis for it,
- how long the data will be stored,
- the recipients of the data, and planned data transfers to a third country,
- the possibility of refusing the processing of their data, or of withdrawing their initial consent, and the implications of such withdrawal,
- the possibility of their data being subsequently processed for a compatible purpose, in accordance with appropriate safeguards provided for by domestic law,
- the specific techniques used for processing their health data,
- the conditions and the means made available to them for exercising via the controller their rights of access, the right of rectification and deletion of their health data, and the possibility to object to the processing thereof.

Comment
According to GDPR article 14.5
.
Paragraphs 1 to 4 shall not apply where and insofar as:
(a) the data subject already has the information;
(b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;

11.2 This information should be provided at the time of data collection or of the first communication, unless it proves impossible or requires disproportionate efforts. It must be appropriate and suited to the circumstances. In particular, where the data subject is physically or legally incapable of receiving the information, it may be given to the person legally representing him/her. If a legally incapacitated person is capable of understanding, he/she should be informed before his/her data are processed.

Comments on the article above
The text should be adjusted so that it corresponds with article 14 in the GDPR.

r.x. 12. Consent

12.2 The results of genetic analyses should be formulated within the limits of the objectives of the medical consultation, diagnosis, ~~or~~ treatment or other purpose for which consent was obtained.

Comment on the article above
This change needs to be done so that an analysis can be done for e.g. research purposes.

s.y. 13. Right of access…
General comment
A comparison is needed here to what is stated about rights in article 15, 16, 17, 20, 21 and 23 in the GDPR plus the right to make exceptions in national law when it comes to usage of data for, scientific or historical research purposes or statistical purposes according to article 89 in the GDPR.

c. the information on the data subject also reveals information on third parties or if, with respect to genetic data, this information is likely to cause serious harm to a ~~consanguine or uterine~~biological relative or to a person who has a direct link with this genetic line; or

d. the data are used for scientific or historical research purposes or statistical purposes where ~~there is no~~denying access to data does not pose an identifiable risk of an infringement of the rights and fundamental freedoms of data subjects, in particular where such data are not used for decisions or measures relating to a specific individual.

Comment on the article above
It is not clear why the recommendation in article 7.4 and 13.5(c) should make a distinction between paternal or maternal relatives when it comes to genetic data. It is difficult to understand what paragraph 13.5(d) aims is at. Should it be read in the way that someone can deny the access to data when it comes to research without risk but not if there is a risk?

13.6 The person subjected to genetic analysis ~~should~~should have the right to be informed of unexpected findings if all of the following conditions are met:

Comment on the article above
It is important from the start that it is clear that the person in question is interested in getting the information. One should have the right to not be informed. Furthermore, it cannot be mandatory to give information, e.g. if it concerns an analysis of many thousands of people during a research study.

---

ii. to a ~~consanguine or uterine~~biological relative, to a member of his/her social family, or to a person who has a direct link with his/her genetic line, unless domestic law provides other appropriate safeguards:

Comment on the article above
See comment above concerning genetic relatives. Why is the uterine relative mentioned here and not the 'agnatic' relative? Biological relative is a more appropriate expression.

Subject to domestic law, the person ~~sh~~could also have the right to be informed if this information is of direct importance to him/her for treatment or prevention.

Comment on the article above
See comment above concerning the right not be informed.

~~t.~~z. Chapter V – Research in the health field

General comment
Research should not be limited to the health field. Health data can be used for other types of research.

~~u.~~aa. 18. Research in the health field

18.1 The use of health data for the purposes of research ~~in the health field~~ must be carried out with a legitimate aim and in full compliance with the principles laid down in this Recommendation.

General comment
Better to use the term 'scientific research' that is used in the text.

18.3 Persons whose data are being used for research ~~must~~ should be informed of such use ~~and~~unless, ~~where~~ exceptions are provided for in domestic law, and give their consent, except if exceptions are provided for in domestic law and in cases of medical emergency.

Comment on the article above

This article should be deleted or changed. There should be a differentiation between processing of personal data with consent as opposed to other types of lawful processing, e.g. if a government agency uses or process data to fulfil a specific task. There should be a possibility to use personal data for research under certain conditions, in both cases.

When the data subject is a legally incapacitated person and domestic law does not authorise the data subject to act on his/her own behalf, his/her legal representative or an authority, or any person or body provided for by law, shall be provided with the information and/or shall give his or her consent in the context of the research project, where such consent is required.

Comment on the article above
Processing of personal data on other grounds than consent should be lawful also in this case.

18.4 The conditions in which health data are processed for research ~~in the health field and, in particular, the value of such data for public health~~ must be assessed by the body or bodies designated by domestic law;

Comment on the article above
We suggest that this paragraph is deleted. We do not understand how this should be set up or who should be supervising this and why? In Sweden and in many other countries there are ethic reviews of research which are done on humans that aims at protecting the individual person and the respect for human values and research.

~~18.5 Subject to additional provisions determined by domestic law, health care professionals entitled to carry out their own medical research should be able to use the health data which they hold as long as the data subject has been informed of this possibility and has not objected.~~

18.6 Personal data used for scientific research may not be published in a form which enables the data subjects to be identified, unless they have given their consent for the publication ~~and~~ or publication is authorised by domestic law.

Comment on the article above
We suggest that paragraph18.5 is deleted. It should not be possible to have exclusive rights to personal data for research just because one has collected it. All research should be examined from an ethic perspective and be treated under the same rules irrespective of if consent is the legal basis for the processing or not!

* * *

AEDH

Recommandation CM/Rec(2016)…. du Comité des Ministres aux Etats membres en matière de protection des données de santé *(adoptée par le Comité des Ministres … 2016, lors de la … réunion des Délégués des Ministres).*

Les Etats sont aujourd'hui confrontés à des enjeux majeurs liés au traitement de la donnée de santé, dont l'environnement a, depuis l'adoption de la Recommandation n° R (97) 5 relative à la protection des données médicales, considérablement évolué.

Cette évolution est due au phénomène de dématérialisation de la donnée rendu possible par l'informatisation du secteur de la santé et à la multiplication des échanges du fait du développement d'internet.

L'informatisation croissante du secteur professionnel et notamment des activités de soins et de prévention, de recherche en sciences de la vie, de gestion du système de santé, et d'autre part l'implication croissante des patients caractérisent notamment ce nouvel environnement.

En outre, les phénomènes de mobilité, le développement des objets et dispositifs médicaux connectés contribuent à de nouveaux usages et à la production d'un volume rapidement croissant de données.

Ce constat partagé par les Etats membres conduit à proposer une nouvelle rédaction de la Recommandation n° R (97) 5 relative à la protection des données médicales, terme auquel on préfèrera le terme plus général de « données de santé », en réaffirmant le caractère sensible des données de santé et l'importance d'encadrer leur utilisation afin de garantir un usage respectant les droits et libertés fondamentales de l'individu notamment le droit au respect de la vie privée.

Le Comité des Ministres, conformément à l'article 15.b du Statut du Conseil de l'Europe, recommande aux Etats membres :

– d'assurer que les principes contenus dans l'annexe de la présente recommandation, qui remplace la Recommandation N° R (97) 5 susmentionnée, sont reflétés dans la mise en œuvre des législations nationales relatives à la protection des données de santé, ainsi que dans d'autres branches de toute loi portant sur l'utilisation des données de santé ;

– d'assurer, à cette fin, que la présente recommandation et son annexe sont portées à l'attention des autorités établies conformément à la législation nationale en matière de protection de données et chargées de contrôler l'application de cette législation, ainsi que des autorités en charge des systèmes de santé ;

– de promouvoir l'acceptation et l'application des principes contenus dans l'annexe de la présente recommandation, au moyen d'instruments complémentaires, tels que des codes de conduite, en s'assurant que ces principes sont bien connus, compris et mis en application par tous les intervenants du secteur de la santé, et pris en compte dans la conception, le déploiement et l'utilisation des TIC dans ce secteur.

ANNEXE A LA RECOMMANDATION CM/REC(2016)…

Chapitre I

Dispositions générales

Objet

La présente Recommandation a pour objet de fournir aux Etats membres des orientations en vue d'encadrer l'utilisation et les différents usages des données de santé afin de garantir le respect des droits et libertés fondamentales de toute personne physique notamment le droit à la vie privée. Elle fournit également les lignes directrices d'un développement de systèmes d'information interopérables et sécurisés permettant d'accroitre la qualité des soins et l'efficience des systèmes de santé.

Champ d'application

La présente recommandation est applicable au traitement de données à caractère personnel relatives à la santé (données de santé) dans les secteurs publics et privés.

Elle définit également les principes de l'échange et du partage des données de santé à l'aide des outils numériques respectueux des droits de la personne et de la confidentialité des données.

Les dispositions de la présente Recommandation ne s'appliquent pas au traitement de données de santé effectué par une personne dans le cadre d'activités exclusivement personnelles ou domestiques.

Définitions

Aux fins de la présente recommandation, les expressions suivantes sont définies ainsi :

- L'expression « donnée à caractère personnel » signifie toute information concernant une personne physique identifiée ou identifiable. Une personne physique n'est pas considérée comme identifiable si cette identification nécessite des délais ou des activités déraisonnables. Lorsqu'une personne physique n'est pas identifiable, les données sont dites anonymes.

- L'expression "données de santé" recouvre toutes données susceptibles de révéler l'état de santé de la personne en relation avec son état physique et/ou mental passé, présent ou futur quelle que soit leur source. Elle concerne également toute information relative à sa prise en charge sanitaire et sociale. Il peut s'agir par ailleurs d'informations de nature biologique et génétique. Sont en outre concernées les données relevant du bien-être et/ou des habitudes de vie dès lors qu'elles révèlent un état de santé.

- L'expression « données génétiques » se réfère à toute donnée relative aux caractéristiques génétiques d'un individu soit héritées soit acquises à un stade précoce du développement prénatal, résultant de l'analyse d'un échantillon biologique de cet individu : analyse des chromosomes, de l'ADN ou de l'ARN ou de tout autre élément permettant d'obtenir des informations équivalentes.

- L'expression "référentiels" désigne un ensemble coordonné de règles et/ou de processus maintenu à l'état de l'art et applicable aux systèmes d'information de santé et qui recouvre les domaines de l'identification, de l'interopérabilité et de la sécurité.

- L'expression "dossier médical électronique" désigne un ensemble sécurisé, structuré ou non, de données de santé d'une même personne qui l'accompagne tout au long de son parcours de soins. Il permet au patient et aux professionnels de santé autorisés de partager les informations utiles à la coordination des soins.

- L'expression "messagerie sécurisée" désigne un service permettant d'échanger de façon sécurisée des données de santé à caractère personnel entre personnes identifiées.

- L'expression "droit à la portabilité " désigne le droit pour les personnes concernées de recevoir les données les concernant confiées à un responsable du traitement, dans un format structuré, et couramment utilisé et de les transmettre, le cas échéant, à un autre responsable du traitement.

- L'expression "applications mobiles" désigne un ensemble de moyens accessibles en mobilité permettant de communiquer et de gérer des données de santé à distance. Elle recouvre des formes diverses comme les objets connectés et les dispositifs médicaux.

- L'expression "professionnels de santé" recouvre tout professionnel reconnu comme tel par le droit national et le droit de l'Union européenne, exerçant dans le secteur sanitaire, médico-social ou social, astreint au secret professionnel et participant à la coordination des soins d'une personne qu'il prend en charge.

- L'expression "hébergement de données de santé" désigne le recours à des organismes tiers pour assurer de façon sécurisée et pérenne la conservation de données de santé sur internet.

- L'expression "anonymisation" désigne le procédé appliqué aux données de santé pour que les personnes concernées ne puissent plus être identifiées ni directement, ni indirectement. L'anonymisation est irréversible.

- L'expression "pseudonymisation" désigne une technique qui permet de rendre une donnée non identifiante aussi longtemps qu'elle n'est pas associée à d'autres éléments conservés séparément et qui permettraient une identification.

- Les notions d'échange et de partage de données de santé qui peuvent caractériser le traitement des données de santé sont définies de la façon suivante. L'échange de données correspond à la communication d'informations à un (des) destinataire(s) clairement identifié(s) par un émetteur connu. Le partage de données permet de mettre des données à la disposition de plusieurs personnes fondées à en connaître selon des principes de droit d'accès sans que ces personnes ne soient nécessairement initialement connues.

- Le terme "communication" signifie toute opération de traitement et notamment l'échange ou le partage de données à caractère personnel permettant de rendre accessibles à des personnes autorisées des données à caractère personnel, quels que soient les moyens ou les supports utilisés.

Chapitre II

Les conditions juridiques d'utilisation des données de santé

Le respect des principes de protection des données à caractère personnel dès la conception (*privacy by design*)

4.1 La personne qui traite des données de santé doit respecter les principes suivants :

g. Le traitement des données doit être proportionné à la finalité légitime poursuivie et ne peut être effectué que sur la base du consentement libre, spécifique, éclairé et non-équivoque de la personne concernée ou en vertu d'autres fondements légitimes prévus par la loi.

h. Les données à caractère personnel doivent être traitées licitement, de façon loyale. Elles doivent être collectées pour des finalités explicites, déterminées et légitimes et ne doivent pas être traitées de manière incompatible avec ces finalités ; le traitement ultérieur à des fins de recherche scientifique ou historique ou à des fins statistiques est compatible avec ces fins, à condition que des garanties complémentaires s'appliquent.

Comment [A191]: Qu'est-ce qui peut garantir que ce traitement ultérieur est compatible avec la finalité de la collecte pour laquelle la personne concernée avait donné son consentement ? ?

i. Les données doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées ; elles doivent être exactes et si nécessaire mises à jour.

j. Les données doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont traitées.

k. Des mesures de sécurité appropriées doivent être mises en place pour empêcher les risques tels que l'accès accidentel ou non autorisé aux données à caractère personnel, leur destruction, perte, utilisation, modification ou divulgation à des tiers non autorisés.

l. Les droits de la personne dont les données sont collectées et traitées doivent être respectés, en particulier son droit d'accès aux données, de communication, de rectification et d'opposition.

4.2 Le traitement de données de santé n'est autorisé que dans la mesure où des garanties spécifiques et appropriées sont prévues par le droit interne afin de prévenir les risques que leur traitement peut présenter pour les intérêts, droits et libertés fondamentales de la personne concernée, notamment un risque de discrimination.

4.3 Les finalités pour lesquelles les données de santé sont traitées doivent également être prises en compte pour permettre un usage pertinent de ces données et adapter en conséquence les garanties.

4.4 ~~En principe, l~~Les données de santé doivent être collectées et traitées par des professionnels de santé, des organismes agissant sous la responsabilité de professionnels de santé ou par les personnes concernées elles-mêmes. Les responsables du traitement et leurs sous-traitants qui ne sont pas des professionnels de santé ne d~~oevrai~~vent collecter et traiter des données de santé que dans le respect de règles de confidentialité et de mesures de sécurité comparables à celles incombant à un professionnel de santé.

4.5 Ces principes de protection des données personnelles doivent être pris en compte et intégrés dès la conception des systèmes d'information collectant, utilisant et exploitant des données de santé. Le respect de ces principes doit être réexaminé régulièrement tout au long de la vie du traitement. Le responsable du traitement doit évaluer l'impact en termes de protection des données et de respect de la vie privée de ses applications.

4.6 Le responsable du traitement doit prendre toutes les mesures appropriées afin de se conformer à ses obligations en matière de protection des données personnelles et doit être en mesure de démontrer en particulier à l'autorité de contrôle compétente que le traitement dont il est responsable est en conformité avec de telles obligations.

5. Le traitement des données de santé

5.1 Le traitement des données de santé doit être effectué de manière loyale et licite et uniquement pour des finalités déterminées.

5.2 Les données de santé doivent ~~en principe~~ être collectées auprès de la personne concernée. Elles ne peuvent être collectées auprès d'autres sources que conformément aux principes 5, 6, 7, 9 et 12 de la présente recommandation, et à condition que cela soit nécessaire pour réaliser la finalité du traitement ou que la personne concernée ne soit pas en mesure de fournir les données.

5.3 Les données de santé peuvent être traitées et communiquées :

~~g.~~j. si la loi le prévoit ou si le traitement repose sur un contrat avec un professionnel de la santé prévoyant des garanties appropriées :

~~ix.~~xiii. aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements ou de gestion de services de santé par les professionnels de santé et du secteur social et médico-social ;

~~x.~~xiv. pour des motifs d'intérêt public dans le domaine de la santé publique comme par exemple, la protection à l'égard de risques sanitaires internationaux ou pour assurer un haut niveau de qualité et de sécurité aux traitements médicaux, produits de santé et dispositifs médicaux ;

~~xi.~~xv. pour des motifs d'intérêt général dans le domaine de la gestion des demandes de prestations et de services de protection sociale et d'assurance maladie ;

~~xii.~~xvi. pour des motifs de santé publique dès lors qu'ils sont licites, légitimes et sont compatibles avec la finalité initiale de collecte des données ;

~~h.~~k. si la personne concernée a donné son consentement conformément au principe 12 de la présente recommandation, sauf dans les cas où le droit interne prévoit qu'une interdiction de traiter les données de santé ne peut être levée par le seul consentement de la personne concernée ;

~~i.~~l. dans la mesure où la loi l'autorise :

~~xi.~~xvi. aux fins de sauvegarde des intérêts vitaux de la personne ou d'une personne incapable physiquement ou légalement d'exprimer son consentement ;

~~xii.~~xvii. pour des motifs tenant aux obligations des responsables du traitement et à l'exercice de leurs droits ou de ceux de la personne concernée dans le domaine de l'emploi et de la protection sociale, dans le respect des règles du droit interne ou de tout accord collectif respectueux de ce dernier et prévoyant des garanties appropriées ;

~~xiii.~~xviii. pour des motifs nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice

~~xiv.~~xix. pour des motifs tenant à la recherche dans le domaine de la santé et du secteur médico-social ;

~~xv.~~xx. pour des traitements à des fins de recherche scientifique ou historique ou à des fins statistiques dans les conditions définies par le droit interne pour garantir la protection des intérêts légitimes de la personne et dès lors que le résultat ne permet pas d'identifier la personne.

Dans tous les cas, des garanties appropriées doivent être mises en place pour assurer en particulier la sécurité des données et le respect des droits de la personne. Toute autre garantie peut être prévue par le droit interne afin de garantir le respect des droits et libertés fondamentales.

6. Données relatives à l'embryon et au fœtus

6.1 Les données médicales relatives à l'embryon et au fœtus, telles que notamment les données résultant d'un diagnostic préimplantatoire, devraient être considérées comme des données à caractère personnel et jouir d'une protection comparable à celle des données de santé d'un mineur.

6.2 A moins que le droit interne n'en dispose autrement, le détenteur des responsabilités parentales peut agir en qualité de personne habilitée juridiquement à agir en tant que personne concernée.

7. Données génétiques

7.1 Les données génétiques traitées à des fins de prévention, de diagnostic, ou à des fins thérapeutiques à l'égard de la personne concernée ou d'une tierce personne (tests génétiques sur des incapables au bénéfice de membres de leur famille par exemple) ou pour la recherche scientifique ne devraient être utilisées qu'à ces seules fins ou pour permettre à la personne concernée de prendre une décision libre et éclairée à leur sujet.

7.2 Le traitement des données génétiques pour les besoins d'une procédure judiciaire ou d'une enquête pénale devrait faire l'objet d'une loi spécifique offrant des garanties appropriées. Ces données devraient servir exclusivement à la vérification de l'existence d'un lien génétique dans le cadre de l'administration de la preuve, à la prévention d'un danger concret ou à la répression d'une infraction pénale déterminée. En aucun cas elles ne devraient être utilisées pour déterminer d'autres caractéristiques qui peuvent être liées génétiquement.

7.3 Tout traitement des données génétiques à d'autres fins que celles prévues aux points 7.1 et 7.2 devrait être autorisé par la loi, en particulier dans les cas où il s'agit de prévenir un préjudice sérieux pour la santé de la personne concernée ou de tiers. En aucun cas, les données génétiques ne peuvent donner lieu à une exploitation commerciale. Le traitement des données génétiques en vue de dépister des maladies peut être autorisé dans l'intérêt vital et dès lors qu'il existe des garanties appropriées définies par la loi.

7.4 La publication de données génétiques permettant d'identifier la personne concernée, un parent consanguin ou utérin de la personne concernée, un membre de sa famille sociale, ou une personne ayant un lien direct avec la lignée génétique de la personne concernée devrait être interdite.

Comment [A192]: Ne faudrait-il pas définir ce que l'on entend par « famille sociale » ?

8. Le secret médical partagé aux fins de prise en charge et d'administration des soins

8.1 Toute personne a droit à la protection de ses données de santé. Dans le cadre de ses relations avec un professionnel de santé, médico-social et social, la personne prise en charge a droit au respect de sa vie privée et au secret des informations la concernant.

8.2 La nécessité d'une plus grande coordination entre professionnels intervenant dans le secteur sanitaire, médico-social et social doit conduire le droit interne de chacun des Etats membres à

reconnaitre un secret professionnel partagé entre des professionnels eux-mêmes astreints au secret professionnel par la loi.

8.3. L'échange et le partage de données de santé entre professionnels de santé doivent être limités aux informations strictement nécessaires à la coordination ou la continuité des soins, à la prévention ou au suivi médico-social et social de la personne, chacun ne pouvant transmettre ou recevoir que les données qui relèvent strictement du périmètre de ses missions.

8.4 La personne concernée doit être informée préalablement de la nature des données collectées et traitées et des professionnels de santé participant à l'équipe de soins. Elle doit pouvoir à tout moment s'opposer à l'échange et au partage de ses données de santé.

9. Communication à des tiers autorisés

9.1 Les données de santé ne doivent pas être communiquées, sauf dans les conditions énumérées dans le cadre de la présente Recommandation.

9.2 Elles peuvent être communiquées à des tiers autorisés par le droit interne à obtenir un accès ponctuel et limité aux données. Il peut s'agir des autorités judiciaires, des experts désignés par une autorité juridictionnelle ou des agents d'une administration désignés par un texte.

9.3 Les médecins de compagnies d'assurance et les employeurs ne peuvent être considérés comme des tiers autorisés à accéder aux données de santé des patients.

10. La conservation des données de santé

10.1 Les données de santé ne doivent être conservées que pour la durée nécessaire à la réalisation des finalités pour lesquelles elles ont été collectées. Le droit interne peut prévoir des durées de conservation précises tenant compte de la nature du support de conservation des données de santé.

10.2 La conservation de données de santé pour des finalités différentes de celles pour lesquelles elles ont été initialement collectées, doit être réalisée dans le respect des principes de la présente Recommandation.

10.3 La personne concernée peut elle-même demander la suppression de ses données à moins qu'elles ne soient rendues anonymes de façon irréversible ou que des intérêts légitimes s'y opposent.

Chapitre III

Les droits de la personne

11. Le droit à l'information

11.1 Toute personne doit être informée de la collecte et du traitement de ses données de santé.

Elle d~~oevrai~~t être informée :

- de l'identité et des coordonnées du responsable du traitement et, le cas échéant, de celle de ses sous-traitants,
- de la finalité du traitement des données et de l'existence, le cas échéant, de son fondement légal,
- de la durée de conservation de ses données,
- des destinataires des données et des transferts de données prévus vers un pays tiers,
- de la possibilité de refuser le traitement de ses données ou de revenir sur son accord initial et des conséquences qui s'y attachent,
- de la possibilité de traiter ultérieurement ses données pour une finalité compatible dans le respect de garanties appropriées prévues par le droit interne,
- des techniques particulières utilisées pour traiter ses données de santé,

- des conditions et des moyens mis à sa disposition pour exercer auprès du responsable du traitement ses droits d'accès, de rectification et de suppression de ses données de santé et de la possibilité de s'opposer à leur traitement.

11.2 Cette information doit être réalisée au moment de la collecte des données ou lors de la première communication à moins que cette information se révèle impossible ou exige des efforts disproportionnés. Elle doit être appropriée et adaptée aux circonstances. En particulier, lorsque la personne est dans l'incapacité physique ou juridique de recevoir cette information, celle-ci pourra être donnée à la personne qui la représente légalement. Si elle est en mesure de comprendre, la personne légalement incapable devrait être informée avant que les données qui la concernent soient traitées.

11.3 L'information de la personne concernée peut être limitée, si la dérogation est prévue par la loi et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique :

à la prévention d'un danger concret ou à la répression d'une infraction pénale,

- pour des raisons de santé publique,
- pour protéger la personne et les droits et libertés des tiers.

11.4 La volonté d'une personne d'être tenue dans l'ignorance d'un diagnostic ou d'un pronostic doit être respectée, sauf lorsque des tiers sont exposés à un risque de transmission. En cas d'urgence médicale, lorsque la vie de la personne est en jeu, les soins priment sur l'information.

11.5 Le droit interne doit prévoir les garanties appropriées de nature à assurer le respect de ces droits.

12. Le consentement

12.1 Lorsque la personne concernée est appelée à donner son consentement au traitement de données de santé, celui-ci devrait être libre, spécifique, éclairé et explicite. Son recueil dès lors qu'il est dématérialisé doit être tracé. Il n'exonère pas celui qui le recueille de ses obligations d'information préalable.

12.2 Les résultats des analyses génétiques devraient être formulés dans les limites des objectifs de la consultation médicale, du diagnostic ou du traitement pour lesquels le consentement a été obtenu.

12.3 Lorsque l'on envisage de traiter des données de santé concernant une personne légalement incapable qui n'est pas en mesure de se déterminer librement, et lorsque le droit interne ne permet pas à la personne concernée d'agir en son propre nom, le consentement de la personne pouvant agir légalement au nom de la personne concernée, ou d'une autorité, ou de toute personne ou instance désignée par la loi, est requis.

12.4 Si la personne légalement incapable a été informée de l'intention de traiter ses données de santé, son souhait devrait être pris en considération, à moins que le droit interne ne s'y oppose.

13. Le droit d'accès, d'opposition et de portabilité

13.1 Toute personne doit pouvoir accéder à ses données de santé directement auprès de la personne qui les détient.

13.2 Le droit d'accès qui emporte le droit de communication des informations, également sur support papier, permet à la personne d'exercer son droit de rectification et d'effacement. Il emporte avec lui le droit de recevoir les données dans un format structuré qui permette de transmettre les données à un autre responsable de traitement désigné par la personne dont les données sont concernées.

13.3 Le droit à l'effacement s'exerce sous réserve des cas prévus par le droit interne invoquant des motifs légitimes. La personne a le droit de s'opposer pour des motifs légitimes à la collecte de ses données de santé à caractère personnel sauf lorsque le détenteur des données invoque une raison impérieuse et légitime qui concerne l'intérêt général de la santé publique.

13.4 En cas de refus de rectifier ou d'effacer les données ou en cas de rejet de l'opposition de la personne concernée, celle-ci doit pouvoir faire recours.

13.5 L'accès aux données de santé peut être refusé, limité ou différé uniquement si la loi le prévoit, et :

~~k.~~e. si cela constitue une mesure nécessaire et appropriée dans une société démocratique à la protection la sécurité nationale, à la sûreté publique, à la prévention, à l'investigation ou à la répression des infractions pénales ; ou

~~l.~~f. si la connaissance de ces informations est susceptible de causer une atteinte grave à la santé de la personne concernée ; ou

~~m.~~g. si l'information sur la personne révèle également des informations sur des tiers, ou, en ce qui concerne les données génétiques, si ces informations sont susceptibles de porter une atteinte grave à des parents consanguins ou utérins, ou à une personne ayant un lien direct avec cette lignée génétique ; ou

~~n.~~h. si les données sont utilisées à des fins de recherche scientifique ou à des fins statistiques et qu'il n'existe aucun risque identifiable d'atteinte aux droits et libertés fondamentales des personnes concernées, notamment du fait que les données ne sont pas utilisées pour des décisions ou des mesures relatives à une personne déterminée.

13.6 La personne soumise à une analyse génétique devrait être informée des découvertes inattendues si les conditions suivantes ont été remplies :

a. le droit interne n'interdit pas une telle information ;

b. la personne a été informée de cette éventualité et a fait la demande explicite de cette information ;

c. l'information n'est pas susceptible de porter une atteinte grave :

i. à la santé de la personne ; ou

ii. à un parent consanguin ou utérin de la personne, à un membre de sa famille sociale, ou à une personne ayant un lien direct avec la lignée génétique de la personne, à moins que le droit interne ne prévoie d'autres garanties appropriées.

Sous réserve du droit interne, la personne devrait également être informée si ces découvertes revêtent pour elle une importance thérapeutique ou préventive directe.

Chapitre IV

Référentiels pour le traitement des données de santé

Le traitement des données de santé doit conduire chaque acteur à un niveau d'exigence élevé pour assurer la confidentialité des données de santé particulièrement sensibles. Les usages qui peuvent en être faits et leur divulgation volontaire ou non exposent les personnes à des préjudices particulièrement importants. Les questions de disponibilité des données (au moment d'un acte médical critique par~~s~~ exemple), d'intégrité et d'auditabilité (dont l'imputabilité) sont par ailleurs tout aussi essentielles.

Dès lors que le recours au numérique conduit à être mieux soigné, ces considérations techniques deviennent éthiques, la disponibilité des données et l'interopérabilité rejoignant la notion de continuité des soins et d'égalité, une absence de réversibilité technique pouvant se traduire en perte d'opportunité de traitement~~e chance~~ pour le malade par exemple.

14. Référentiels

14.1 Conformément au principe de privacy by design tel que défini au point 4.5, les applications qui gèrent des données de santé doivent intégrer dès leur conception les principes de protection des données personnelles et les référentiels de sécurité et d'interopérabilité et s'assurer de la conformité de leur traitement à ces principes et référentiels.

14.2 Ces référentiels ont pour objet, en fonction des usages, de définir de façon coordonnée avec les acteurs les conditions d'usages des données de santé dans les systèmes d'information afin d'assurer leur confidentialité et leur interopérabilité. Ils recouvrent les domaines de l'identification, de l'interopérabilité et de la sécurité.

15. Les référentiels d'interopérabilité

15.1 Ces référentiels spécifient les standards à utiliser dans les échanges et lors du partage des données de santé entre systèmes d'information de telle façon qu'un produit ou un système informatique puisse fonctionner avec d'autres produits ou systèmes existants ou futurs. Ils impliquent l'utilisation d'un langage commun (interopérabilité sémantique) et des référentiels techniques (interopérabilité technique) communs.

15.2 Pour garantir aux personnes concernées le respect de leurs droits et permettre le développement de systèmes d'information efficients, les professionnels de santé et les patients ainsi que tout organisme autorisé à traiter des données de santé, notamment les personnes responsables des plateformes permettant l'échange et le partage des données de santé, doivent respecter des règles de sécurité et des référentiels auxquels le droit interne de chaque pays peut donner une force juridique par exemple en recourant à un procédé de certification et qui doit conduire à leur acceptabilité par l'ensemble des acteurs. Leur respect doit en particulier être assuré, dès lors que les données de santé sont collectées et traitées dans le cadre des relations de prise en charge et de soins.

15.3 Ces référentiels ont pour objet de définir des standards permettant l'échange et le partage des données de santé par les systèmes d'information et d'assurer le suivi de leur mise en œuvre dans des conditions de sécurité requises.

15.4 Ils sont fondés sur les principes suivants :

~~j.~~g. utiliser un langage et des formats communs de contenus partagés ou échangés fondés sur des standards communs (interopérabilité sémantique) ;

~~k.~~h. recourir à des services interopérables et à des règles d'utilisation communes ;

~~l.~~i. utiliser pour le transport des données, des protocoles d'interconnexion et d'acheminement de l'information sécurisés ;

~~m.~~j. garantir aux personnes concernées une identification fiable afin d'assurer l'unicité de leur identité au sein des différents systèmes d'information. L'identifiant retenu doit être unique,

univoque, pérenne et reconnu par l'ensemble des acteurs et fondé sur un dispositif de certification fiable ;

~~n.~~k. assurer l'authentification des personnes et des systèmes qui interviennent dans le traitement des données à l'aide de dispositifs reconnus par l'ensemble des acteurs et de nature à garantir la sécurité de l'échange et du partage des données ;

~~o.~~l. utiliser des solutions sécurisées telles que définies au Principe 16.

16. Les référentiels de sécurité

16.1 Le traitement des données de santé doit être sécurisé et recourir à des solutions qui garantissent la disponibilité, l'intégrité, la confidentialité et l'auditabilité des données.

16.2 Ces règles de sécurité, maintenues à l'état de l'art, doivent se traduire par l'adoption de mesures techniques et organisationnelles de nature à protéger les données de santé contre toute destruction illégale ou accidentelle, toute perte, toute altération et de prévenir tout accès non autorisé. En particulier, le droit interne doit prévoir d'organiser et d'encadrer les modalités de collecte, de conservation et de restitution des données de santé.

16.3 La disponibilité - c'est-à-dire le bon fonctionnement du système - doit être assurée par des mesures de nature à rendre accessibles les données de façon sécurisée et dans le respect des habilitations de chacun.

16.4 Le respect de l'intégrité impose de vérifier toute action effectuée sur la nature des données, leur modification éventuelle et leur effacement, y compris lors de la communication des données.

16.5 La confidentialité des données se traduit par la mise en place de mesures destinées à contrôler les accès aux serveurs de données et aux données elles-mêmes en s'assurant que seules les personnes autorisées puissent accéder aux données.

16.6 L'auditabilité doit conduire à disposer d'un système permettant de tracer tous les accès au système d'information et de pouvoir imputer à une personne les actions qu'elle a effectuées.

16.7 L'activité qui consiste à conserver sur internet des données de santé et les rendre disponibles pour le compte des utilisateurs doit être réalisée dans le respect des référentiels de sécurité et des principes de protection des données personnelles.

16.8 Des professionnels non impliqués directement dans la prise en charge sanitaire de la personne mais assurant au titre de leurs missions le bon fonctionnement des systèmes d'informations, peuvent accéder dans la mesure indispensable à l'accomplissement de leurs tâches et de façon ponctuelle aux données de santé. Ils doivent respecter le secret professionnel et toutes mesures appropriées prévues par le droit interne pour garantir la confidentialité et la sécurité de ces données.

17. Les services de gestion des données de santé

17.1 Chaque Etat membre devrait mettre en place les services d'échange et de partage des données de santé, supports utiles en particulier à la coordination des soins et respectueux des référentiels définis aux principes 14 à 16. Dès lors que ces capacités d'échange et de partage contribuent à la qualité des prises en charge comme à la bonne gestion des systèmes de santé et autres finalités, au service tant des individus que de l'intérêt général et de la santé publique, chaque professionnel de santé et du secteur médico-social et social doit disposer d'un dispositif de gestion dématérialisée de son activité le mettant en capacité d'échanger ou de partager les données de santé des personnes.

17.2 Les patients doivent pouvoir bénéficier d'un dossier médical électronique sécurisé qui leur permet de disposer des informations utiles à leur suivi médical, médico-social et social tout au long de leur parcours de soin. Les informations de ce dossier médical peuvent avec l'accord du patient être partagées par les professionnels intervenant dans la prise en charge de la personne dans les conditions définies au principe 8.

17.3 Tout système de messagerie électronique permettant l'échange de données de santé doit respecter les référentiels définis dans le présent Chapitre.

Chapitre V

La recherche dans le domaine de la santé

18. La recherche dans le domaine de la santé

18.1 L'utilisation des données de santé à des fins de recherche scientifique dans le domaine de la santé devrait être effectuée dans un but légitime et dans le respect des principes posés dans la présente Recommandation.

18.2 La nécessité du recours à des données de santé doit être appréciée au regard de la finalité poursuivie.

18.3 Les personnes concernées par l'utilisation de leurs données de santé pour la recherche doivent être informées de cet l'usage ~~de leurs données~~ et, quand le droit national le prévoit, consentir à cet usage sauf en cas d'urgence sanitaire. Lorsque la personne concernée est légalement incapable et que le droit interne ne lui permet pas d'agir en son propre nom, son représentant légal ou une autorité, ou toute personne ou instance désignée par la loi, recevra l'information et/ou donnera son consentement dans le cadre du projet de recherche.

18.4 Les conditions de traitement des données de santé à des fins de recherche dans le domaine de la santé et en particulier leur intérêt pour la santé publique doivent être appréciées par un ou plusieurs organismes désignés par le droit interne.

18.5 Sous réserve de conditions complémentaires prévues par le droit interne, les professionnels de santé habilités à mener leurs propres recherches médicales devraient pouvoir utiliser les données de santé qu'ils détiennent pour autant que la personne concernée ait été informée de cette faculté et ne s'y soit pas opposée.

18.6 Les données à caractère personnel utilisées à des fins de recherche scientifique ne peuvent être publiées sous une forme permettant d'identifier les personnes concernées à moins que ces dernières n'aient donné leur consentement en vue de la publication et que le droit interne autorise cette publication.

Dans tous les cas, des garanties appropriées doivent être mises en place pour assurer en particulier la sécurité des données et le respect des droits de la personne. Toute autre garantie peut être prévue par le droit interne afin de garantir le respect des droits et libertés fondamentales.

Chapitre VI

Les dispositifs mobiles

19. Les dispositifs mobiles

19.1 Le développement d'applications mobiles permet aux personnes concernées comme aux professionnels du secteur de la santé et du secteur médico-social et social de collecter et traiter à distance des données de santé. Ce développement revêt des formes diverses et recouvre plusieurs catégories d'applications qui elles-mêmes poursuivent des finalités d'usage très différentes. Du dispositif médical aux applications de "mesure de soi" (quantified self), ces objets connectés permettent de quantifier et/ou d'évaluer des paramètres susceptibles de révéler l'état de santé d'une personne et sont dans certains cas utilisés directement pour poser des diagnostics et délivrer des soins.

19.2 Dès lors que les données collectées par ces applications sont susceptibles de révéler l'état de santé d'une personne, concernent toute information relative à sa prise en charge sanitaire et sociale et/ou sont traitées dans un contexte médical, elles constituent des données de santé. A ce titre elles doivent bénéficier des mêmes protections juridiques et de confidentialité que celles applicables aux autres modes de traitements de données de santé telles que définies par la présente Recommandation et, le cas échéant, complétées par le droit des Etats.

19.3 Les applications de bien-être ou de "mesure de soi" utilisées pour le seul bénéfice de la personne qui l'utilise, mises en œuvre à des fins exclusivement personnelles et qui ne donnent pas

lieu à une communication extérieure ne devraient pas être considérées comme soumises aux exigences de la présente Recommandation. Des orientations sur l'application des principes de protection des données au traitement de données de santé, au moyen de ces applications mobiles, par des entités du secteur privé sont à prévoir dans un document distinct de la présente Recommandation. *********

BIOETHICS COMMITTEE / COMITÉ BIOÉTHIQUE (DH-BIO)

Cyprus

The draft recommendation has the full agreement and support of the Cyprus National Bioethics Committee and there are no further comments to make.

Finland

The Government makes the following comments on the draft Recommendation, in the order of the provisions in the draft:

Paragraph 4 ”Privacy by design”

The heading could also mention ”privacy by default”.

Paragraph 5.2: *"Health data shall in principle be collected from the data subject. They may be collected from other sources only if in accordance with principles 5, 6, 7, 9 and 12 of this Recommendation and if this is necessary to achieve the purpose of the processing or if the data subject is not in a position to provide the data."*

The reference to the principles leaves it unclear what they relate to. It also remains unclear how “in principle” should be interpreted.

Paragraph 5.3: *"for processing for statistical, historical or scientific research purposes under the conditions defined by domestic law to guarantee protection of the data subject's legitimate interests and where the individual cannot be identified from the results".*

It is important to ensure that this will not preclude the use of the data later, e.g. in follow-up research, although the individual cannot be identified from the results. Moreover, it is advisable to state that statistical or research purposes are not considered to conflict with the original purpose of use, in order that the data can be used for these purposes, if necessary, even if they had originally been collected for another purpose.

Paragraph 6.1: *"Medical data concerning embryos and foetuses, inter alia, such as data resulting from a pre-implantation diagnosis, should be considered as personal data and enjoy protection comparable to the protection of the health data of a minor."*

It remains unclear who owns the data and makes the decisions concerning them, if embryos and foetuses have the said rights. The consent for using the data will probably be requested from the mother, although there are other possible parties, too (father, donor); if a child is born, will the decision-making power be transferred to him or her at some stage?

Chapter VII

According to the draft Recommendation, an informed consent is required for the processing of data. The applicability of this provision to genome research is challenging, considering that the result or unexpected information is not necessarily predictable

Paragraph 7.1: "*or for scientific research should be used only for these purposes or to enable the data subject to take a free and informed decision on these matters".*

For instance in genome research, which may concern many members of families, account should also be taken of the rights of persons other than the researched ones; this has been taken into consideration to some extent in paragraph 7.3.

Chapter III (paragraphs 11 to 13.6)

Issues related to the rights of data subjects should be assessed against the question what the Data Protection Regulation stipulates on the rights of data subjects and on the possibility of restricting these rights. In addition to the rights mentioned in the draft Recommendation, the Regulation also provides for e.g. the right to restriction of processing (Article 18) and automated individual decision-making, including profiling (Article 22).

Paragraph 13.6 (b): "*the person himself or herself has asked for this information"*.

The provision leaves it unclear how to act in situations where the person has not understood that he or she could ask for the information. It also remains unclear whether third parties whose information may be disclosed in research have the right to receive information or the right to refuse to receive information.

Chapter V

For a long time, health research and statistics in Finland and the other Nordic countries have been based on the collection of data for the national population registers and other data files. The data thus collected have been used successfully also in research as well as in planning and studies by authorities. Confidential and sensitive data used by social welfare and health care services have been collected on a statutory basis in nation-wide personal data files without any consent of the data subjects. The draft Recommendation seems to focus on digital patient documents, on which some of the data collected for the files are, however, based.

In conducting scientific research, the consent of the researched person is, of course, always of primacy, but departures from the requirement of the consent have been permitted if the consent has not been available on account of the large amount of the data, the person's age or a similar reason and if the preconditions laid down in law are met (Section 14 of the Finnish Personal Data Act). Health research on data recorded in data files is usually based on extensive materials describing the whole population of the country, and in such cases it has been permissible to depart from the requirement of the consent. It has also been possible to use patient documents for research purposes by the same principles as in research on data from data files. However, for research on documents or on data from data files, a permit to use these sources must be requested from the responsible authority. From the standpoint of research ethics, no major ethical challenges have been identified in research on documents or on data from data files, when the requirements laid down by law are complied with.

Paragraph 18.3: "*Persons whose data are being used for research must be informed of such use and, where provided for in domestic law, give their consent, except in cases of medical emergency".*

This requirement would have negative effects on research on data from data files and would in practice prevent sensible research of this kind if the research could not be conducted without the consent of the data subjects. The consent and the provision of information have been expressed as a categorical point of departure for all processing of health data, without taking into account exceptions that are important from the national and public health perspective. Moreover, the Recommendation is internally contradictory: according to paragraph 5.3, health data could be used for research and statistics if the processing of the data is provided for by law. The Recommendation should at least be internally consistent.

The Recommendation requires a strong linkage with the purpose of use of the data and the related needs. This is challenging from the standpoint of the national requirements for the duration of storage and must be examined in that context. For instance, the right of a person to demand that their data be deleted is linked with the purpose of use of the data.

Comments by the Finnish data protection Ombudsman

The Data Protection Ombudsman commends the fact that the draft Recommendation of the Council of Europe on the protection of personal health data is consistent with the digital developments in society. As any other personal data, also health data must be handled as confidential, by observing information security and respecting the will of the individuals in question and their right to self-determination.

The Data Protection Ombudsman considers it advisable to take account of Regulation (EU) 2016/679 of the European Parliament and of the Council, "the General Data Protection Regulation", in the ongoing preparation of the draft Recommendation. According to its Article 99, the Regulation shall apply from 25 May 2018. It is particularly important to ensure that the Regulation and the present draft Recommendation of the Council of Europe, both of them legally binding, will not conflict with each other. In respect of the EU Member States, a major part of the issues addressed in the draft Recommendation are also covered by the EU Data Protection Regulation. The Recommendation should be confined to the conditions laid down in the Regulation.

The purpose and context of the Recommendation remain remote and unclear in some respects. The essential content of the Recommendation can already be found in legislation and in international and national instructions. Although the Recommendation should be applicable in the whole Europe, its text does not always recognise the special features of different countries.

Paragraph 3

According to the definition of pseudonymisation, pseudonymised personal data, which could be associated with a natural person by using other elements, should be considered as *data of an identifiable natural person, i.e. as personal data*.

The Recommendation uses the concepts of *controller* and *processor* but does not define them.

Paragraph 5.1

From the perspective of the General Data Protection Regulation, particularly special questions concerning the national margin of appreciation must be taken into account in respect of the legal basis for the processing of personal data. The processing of health data must be justifiable by some of the legal bases provided for in Articles 6 and 9 of the Regulation. Under the Regulation, personal health data fall in a special category of personal data and are thus in principle covered by the prohibition of processing.

Paragraph 8.1

For the processing of personal health data it is particularly important to define those actors who have the right to process them. Each employee may only have access to those data files and data which relate to their work duties. This is a key guarantee of legal protection for both the data subjects and the health care and/or social welfare professionals.

France (under translation)

Le projet de Recommandation du T-PD en matière de protection des données de santé suscitent plusieurs interrogations et observations de la part de la délégation française.

En effet, le projet de Recommandation porte sur les droits des personnes (droit a la vie privée, consentement, information de l'usage), l'utilisation des données de santé sensibles pour des finalités diverses, l'encadrement des examens génétiques, question particulièrement délicate (exemple : médecine prédictive) et enfin la recherche. Or il s'agit de sujets qui relèvent des principes issus des travaux du DH-BIO : Convention d'Oviedo, Protocole recherche, Protocole génétique, Recommandation sur l'utilisation des données associées aux collections d'échantillons biologiques a des fins de recherches, Recommandation sur génétique et assurance et qui, à ce titre, nécessitent d'être examinés à la lumière de ces textes afin d'assurer une cohérence d'ensemble.

***

Sur un plan général, ce document normatif, même s'il n'est pas contraignant s'agissant d'une Recommandation, n'a pas toujours la rigueur rédactionnelle et la précision juridique souhaitables (certains passages relèvent plus de l'exposé des motifs que de l'écriture normative et les termes utilisées ne sont pas suffisamment définies...). Les textes précités du champ bioéthique devraient servir de référence et pourraient offrir les définitions manquantes.

Introduction p 3

- 4eme § : certains termes utilisés ne sont pas suffisamment définis empêchant ainsi de déterminer le champ qu'ils entendent couvrir. Ainsi, qu'entend-ton par « *phénomènes de mobilité* » : s'agit-il des problématique liées à l'utilisation des téléphones mobiles ou plus largement aux pratiques médicales à distance ?

  De même, la référence aux « *objets et dispositifs médicaux connectés* » exclut-elle les objets non médicaux ? Dans l'affirmative qu'en est- il des objets non médicaux mais utilisés à des finalités médicales ?

Chapitre I

- Objet (p3-4) : il s'agit, selon le projet de Recommandation d'encadrer « *l'utilisation et les différents usages* ». Ces deux termes proches, devraient être définis plus précisément par le T-PD s'il estime qu'il existe entre ces deux termes une différence et qu'ils recouvrent deux situations différentes. Une telle précision s'avère nécessaire pour déterminer le champ de la Recommandation.

Chapitre II

- Point 4

La définition du consentement et ses différentes modalités ne sont pas clairement précisées. Or, selon le type de données ou la finalité du traitement (ex : recherche, études..), il peut s'agir d'un consentement exprès, spécifique et écrit ou d'un droit d'opposition après information. Ce point devrait être mieux articulé avec les principes posés au chapitre III relatifs aux droits portant sur l'information et le consentement.

Enfin, au point 4.4, il conviendrait de clarifier le rôle et les responsabilités des différents acteurs. Si la collecte et le traitement peuvent être confiés à des non professionnels de santé (techniciens, épidémiologistes, statisticiens…), dans tous les cas le respect de la confidentialité et du secret professionnel, ou médical selon le cas, doit être garanti.

- Point 5

Quelle est l'articulation de ce point avec les principes posés au point 4 ?

De façon générale, il est très difficile de savoir lorsque la recommandation s'attache aux données personnelles dans le cadre d'une prise en charge individuelle ou lors que la finalité est « collective », de recherche ou santé publique.

Ainsi, il conviendrait de clarifier la présentation du point 5 dans son ensemble : par exemple les points 5.3 a), b) et c) sont-ils cumulatifs ?

- Point 6

Le statut juridique du fœtus et de l'embryon n'est pas reconnu dans l'ensemble des Etats membres du Conseil de l'Europe et notamment en France. La Cour européenne des droits de l'homme énonce qu'il n'est « *ni souhaitable ni même possible actuellement de répondre dans l'abstrait à la question de savoir si l'enfant à naître est une personne au sens de l'article 2 de la Convention* » (Cour EDH, 8 juillet 2004, *Vo c. France*) et laisse, en conséquence, une totale liberté aux Etats sur ce sujet.

Dans un arrêt de Grande chambre du 27 août 2015, *Parillo c. Italie*, la Cour a considéré, dans une affaire de don d'embryons, que ceux-ci renfermant le patrimoine générique de la mère et constituant une partie de son identité, elle est fondée à agir au regard du droit au respect de la vie privée (garanti

par l'article 8 de la Convention) et que les Etats disposaient d'une ample marge d'appréciation sur le sujet du statut de l'embryon en l'absence de consensus européen.

En outre, le point 6.2 énonce que le détenteur des responsabilités parentales peut agir en qualité de personne habilitée juridiquement à agir en tant que personne concernée. La notion de « détenteur des responsabilités parentales » soulève des difficultés au regard du droit national français et n'est pas applicable à l'embryon ou au fœtus. Dès lors, il faudrait parler du « couple » dont l'embryon est issu.

Par ailleurs, si on évoque à ce point le diagnostic préimplantatoire (DPI), il ne peut s'agir d'un fœtus, le DPI n'étant possible que sur un embryon in vitro. Ici encore l'embryon ou le fœtus ne peuvent être considérés comme une personne (mineure). Ces dispositions pourraient être intégrées sous une autre forme dans le point 4 afin de préciser ce qu'il en est pour les données personnelles recueillis avant la naissance et traitées ultérieurement, sur l'enfant ou la personne adulte.

- Point 7

Sur les **données génétiques**, le projet de Recommandation ne distingue pas les données selon qu'elles sont ou non prédictives et les modalités du consentement qui peuvent être différentes ne sont jamais précisées.

Au point 7 .1 : l'intérêt de la personne, du tiers apparentés et celui de la recherche ne peuvent être mis sur le même plan s'agissant du consentement.

Le point 7.2 est confus, la dernière phrase est d'interprétation difficile. Veut-on évoquer les problèmes tenant à l'utilisation de données génétiques médicales à des fins non médicales (par exemple pour identifier une personne dans le cadre judiciaire) ? La question de la différence entre identification et expression pathologique d'un gène, entre gène codant ou non codant pourrait être exposée ici.

Que recouvre le point 7.3 ? Quelle finalité autre que la finalité préventive, diagnostic ou thérapeutique ? Ce point semble incomplet. S'agit-il de faire référence à l'utilisation des données dans le cadre de l'assurance ou de l'emploi ?

Au point 7.4 : la référence à la « famille sociale » n'a pas de sens du point de vie génétique et que veut-on dire par « parent consanguin ou utérin », cet expression devrait être précisée. De manière plus générale, quelle est la portée exacte de ce point ?

- Point 8

Le point 8.2 n'est pas normatif et il conviendrait de clarifier l'apport du point 8.3 par rapport au 8.2. En effet, le le second limite ce que le premier ouvre.

- Point 9

Le droit à communication est-il complet ? Certains acteurs ne sont-ils pas oubliés, par exemple la recherche ? Plus de précisions permettrait de mieux envisager les garanties nécessaires.

- Point 10

Cette partie mériterait d'être davantage précisée quant au changement de finalité et le point 10.3 relève davantage du chapitre III

Chapitre III

- Point 11

Cette partie porte sur l'information relative à la conservation et au traitement des données personnelles. Aussi le point 11.4 apparait confus en ce qu' il aborde la question du droit d'être tenue dans l'ignorance d'un diagnostic, ce droit relevant du droit d'information sur l'état de santé dans le cadre de la relation médecin-malade.

- Point 12

Cette partie porte sur le consentement et appelle des remarques identiques à celles formulées au point précédent : des confusions sont à clarifier notamment selon que l'on se situe dans l'obtention des données, leur conservation ou leur traitement.

La question du rendu des résultats et du consentement à l'examen des caractéristiques génétiques est d'un autre ordre que le consentement au traitement de données. Ainsi, le recueil du consentement au « traitement », sans précision de la finalité de ce traitement, apparait flou. La collecte des données, qui est visée au point précédent est-elle également concernée par ce point ?

En conséquence, les modalités du consentement selon les situations (finalité de recherche par exemple) et le type de données (prédictives ou non) devraient être davantage précisés.

Par ailleurs, il n'est pas précisé que le consentement doit être donné par écrit, ce qui parait pourtant nécessaire en termes de preuve.

Enfin, au point 12.3 on cible dans la même phrase la personne incapable juridique et qui n'est pas en mesure de se déterminer, les 2 conditions ont-elles cumulatives ?

En outre, ce point vise-t-il seulement les majeurs incapables ou également les mineurs ? Si tel est le cas, il faudrait alors l'indiquer expressément et ne pas se référer à la capacité de se déterminer librement. En effet, en droit interne, un mineur, même doté de discernement, est incapable juridiquement et doit être représenté.

- Point 13

Le point 13.5 n'est pas très lisible et devrait être clarifié. Les finalités pourraient être distinguées afin d'éviter le cumul de conditions et sous conditions.

Le point 13.6 relève de l'encadrement de l'information préalable à un examen des caractéristiques génétiques d'une personne dans le cadre d'une prise en charge médicale et non du traitement des données médicales.

Chapitre IV

Dans l'introduction à ce chapitre, outre le fait que les deux paragraphes ne sont pas normatifs, le 2ème alinéa qui semble dire que le recours pour mieux soigner « au numérique » est de facto « éthique », pose questions. A cet égard, ne conviendrai-il pas mieux de rappeler simplement le respect des principes de nécessité et de proportionnalité ou encore de rappeler la notion de balance bénéfice /risque ?

En outre le projet de Recommandation devrait définir ce qu'il entend viser par l'expression « au numérique ».

Chapitre V

Ce chapitre qui porte sur la recherche dans le domaine de la santé pourrait être rédigé en s'appuyant sur les principes de la convention d'Oviedo et le Protocole additionnel sur la recherche et recommandation sur les biobanques. Il s'agit d'un chapitre important qui doit être approfondi et clarifié.

Chapitre VI

Comme le chapitre V, ce chapitre semble en tout état de cause inachevé tant il est peu précis voire peu normatif mais plutôt descriptif de situations.

Germany

The recommendations on protecting health data still seem to require further development. Furthermore, they are not consistent with the rules of the EU's General Data Protection Regulation

(GDPR), for example with regard to definition of terms, preconditions for consent for processing of health data, and the rights of affected persons. Also, it is not made adequately clear whether health data is to be protected in general terms (title, purpose, scope) or if the recommendation covers only protection within the scope of health care. This urgently requires clarification. Additionally, compared with the other recommendations, the text has a very prescriptive character, so that it seems necessary to fundamentally rework the recommendation based on the GDPR and Convention 108, which is still in the process of being concluded. Likewise, the language of the recommendation should be phrased so that possible contradictions in interpreting the recommendation, Convention 108, and the GDPR can be excluded. Continued substantive discussion on the recommendation – in particular with respect to its adoption – should be postponed until after the conclusion of Convention 108.

Ireland

General Remark

In terms of data protection definitions and concepts, it would be helpful to everyone to have consistency between the EU and C of E.

Preamble

This changed environment is due to the phenomenon of data digitisation, made possible by the computerisation of the health sector and to the proliferation of exchanges arising from the development of the Internet. As well as by the changing attitudes of data subjects to wanting greater control over who processes their personal health data and for what purposes.

Noteworthy features of this new environment are the growing computerisation of the professional sector and particularly of activities relating to care and prevention, to life sciences research and to health system management, and also the increasing involvement of patients.

Besides, mobility and the development of connected medical objects and devices contribute to new uses and to the production of a rapidly growing volume of data.

Rq: Internet of Things? Develop further given its increasing importance.

Chapter I

Scope

This Recommendation is applicable to the processing of personal data relating to health (health data) in the public and private sectors, including voluntary sectors.

The provisions of this Recommendation do not apply to health data processing performed by individuals in the context of exclusively personal, family or domestic activities.

Definitions

- The expression “personal data” refers to any information relating to an identified or identifiable living individual.

- It may shall? also involve information of a biological and genetic nature. It further covers data relating to well-being and/or lifestyle where these reveal a state of health.

- The expression “genetic data” refers to any data relating to an individual's genetic characteristics, whether inherited or acquired at an early stage of prenatal development, resulting from the analysis of a biological sample from that individual: analysis of chromosomes, DNA or RNA or any other component making it possible to obtain equivalent information.

Rq:Limited but essentially consistent with EU.

- The expression “health professionals” covers all professionals recognised as such by national and European Union law practising in the health, medical welfare or social welfare sector, bound by professional secrecy and involved in co-ordinating treatment for an individual to whom they provide health care. Are they using “social welfare” in a different context from what we would understand?

- The concepts of exchange and sharing of health data, which can be features of health data processing, are defined as follows:

(b) Data sharing enables data to be made available to several persons entitled to be made aware of such data according to the principles of the right of access (Rq: I am not sure I understand what is meant here principles of the right of access but it seems different from data subject access rights), without these persons necessarily being known at the outset.

Chapter II

4.1 Anyone processing health data must comply with the following principles:

~~v.~~bb. Personal data must be processed transparently, lawfully and fairly. They must be collected for explicit, specified and legitimate purposes and must not be processed in a manner that is incompatible with these purposes; subsequent processing for scientific or historical research purposes or statistical purposes is compatible with those purposes on condition that additional guarantees apply.

e. The rights of the person whose data are collected and processed must be respected, particularly their rights to know that data is being held about them, of access to the data, communication, rectification and objection.

4.2 The processing of health data is permissible only insofar as specific and appropriate guarantees are provided for in domestic law (by legislation or otherwise) to prevent any risk to the interests, rights and fundamental freedoms of the data subject which the processing may represent, in particular the risk of discrimination.

5.1 Health data must be processed transparently, fairly and lawfully and only for specified purposes.

6.1 Medical data concerning embryos and foetuses, *inter alia* such as data resulting from a pre-implantation diagnosis, should be considered as personal data and enjoy protection comparable to the protection of the health data of a minor.

Rq: This is a tricky issue that legal advice should be obtained on.

7.4 The publication of genetic data which would identify the data subject, a consanguine or uterine relative of the data subject, a member of his/her social family or a person who has a direct link with his/her genetic line, should be prohibited unless expressly permitted by law with appropriate safeguards.

Chapter III

13.5 Access to health data may be refused, limited or delayed only if the law provides for it and if:

d. the data are used for scientific or historical research purposes or statistical purposes where there is no identifiable risk of an infringement of the rights and fundamental freedoms of data subjects, in particular where such data are not used for decisions or measures relating to a specific individual.

Rq: This doesn't seem like a good idea. Data subjects should have access to their health data when it is held by a researcher.

Chapter V - Research in the health field

18.3 Persons whose data are being used for research must be informed of such use and, where provided for in domestic law, give their consent, except in cases of medical emergency.

Rq: This seems at variance with the EU DP Regulation.

18.5 Subject to additional provisions determined by domestic law, health-care professionals entitled to carry out their own medical research should be able to use the health data which they hold as long as the data subject has been informed of this possibility and has not objected.

Rq: Is this a continuation of the *traditionally understood* distinction between a GP using his or her patients' medical records for his or her own research project as contrasted with the situation where the GP discloses such information to a third party researcher. The EU DP Regulation does not appear to make that distinction.

18.6 …Any other guarantees may be provided for in domestic law with a view to safeguarding respect for rights and fundamental freedoms.

Rq: Is the notion of broad consent captured?

Switzerland

- The recommendation fails to clarify the question of whether only data resulting from the genetic analysis of health-relevant characteristics are to be processed (as the title of the recommendation would suggest), or whether the definition as per the third paragraph of point 3 applies. This, for example, would also cover data resulting from DNA profiles to clarify parentage or genetic data on questions such as a person's aptitude for endurance sports, character traits, etc. For us the relationship between the definitions of "health data" and "genetic data" seems unclear.

- Even though the definition given for genetic data is on the one hand very open, in another respect it is narrow and diverges from the terms of the new EU Data Protection Regulation (Art. 4 point 13): When it comes to acquired characteristics not all data are processed, but only those acquired at an early stage of prenatal development. So data from the genetic analysis of tumour tissue are not processed. Why does the recommendation diverge from the EU regulation, which does not narrow the definition down to "an early stage of prenatal development"?

- Point 6 leaves a number of questions open: What is the reasoning behind this recommendation? Is the implication that the foetus is accorded specific personality rights that are exercised by the holders of parental responsibilities? Does this mean that the father also has corresponding rights even though (at least in our understanding of the law) only the mother decides on the conduct of prenatal examinations? What happens in the event of a stillbirth or miscarriage? Do the requirements apply only for the duration of the pregnancy or also subsequently?

- Given the fact that data per se can be commercialised, the absolute ban on commercial exploitation (point 7.3) leaves a number of questions open: What is meant by "commercial exploitation"? Does the ban also apply in the context of commercial research? Why should genetic data (with the consent of the person involved) not be commercially exploited?

- Point 12.2 only makes sense in a health-relevant context. However, the definition of genetic data in point 3.3 goes beyond the health-relevant context (see our first point above). We believe that clarification is needed here.

- Points 13.5 b) and 13.6 c) imply a paternalistic approach that we do not believe is what should be striven for these days. Point 13.6, and particularly point b), demonstrates this tension very clearly. We believe that only the consideration mentioned in this b) – the will of the person affected – should be the sole deciding factor. This person should be told in advance that certain information may have serious consequences. But they should decide for themselves whether they want to be informed.

- When it comes to research (point 18), it must be made clear that domestic law has precedence (as, for example, in point 18.3). This proviso probably also applies to point 18.5, but the way it is formulated – at least in the French version – differs (the English version seems to be clearer). In any case more stringent domestic law must have precedence (for example if it requires consent as opposed to mere dissent).

United Kingdom

9.1. We are grateful for an opportunity to comment on the draft recommendation on health data as this is a sensitive area that requires a careful balance between the protection of individual patient data whilst recognising the complex landscape of modern health and care organisations. It is important to recognise that over-protecting patient information can be detrimental to patient care and can interfere with the rights of the individual.

10.2. In the limited time available it has not been possible to make detailed comments on the text and it would be sensible to assume that there will be a thorough editorial process to ensure that terms are used consistently and that the terminology is accessible to those working in English.

11.3. There are also number of areas where the intention of the drafting is not clear such that we are not able to make any proposals for changes to the text. This is particularly important in relation to the intention behind the sections on genetic data where the linkages between genetic data and between members of a social family are hard to fathom. An example of the rather opaque drafting here is in para 13.5c – is it necessary to set out consanguineous, uterine or direct link to the genetic line or could this simply be phrased as "reveals information about third parties including genetic relatives"?

12.4. In section 7.3 a complete prohibition of commercial exploitation is not workable given the complex interplay of commercial and non-commercial actors in healthcare (in the UK all family doctors and pharmacists are effectively small businesses.) The text in section 5.3 is appropriate in this respect and there should be some cross-reference to the principle of contractual safeguards.

13.5. In section 7.4 on the publication of genetic data also has the drawback of prohibiting legitimate scientific publication in cases of rare disease. Often these will include enough information – or even images that self-identification possible. In many cases patients give consent for images to be published alongside case descriptions given that these are highly relevant to other clinicians. It may be necessary to cross-reference with 18.6.

14.6. Section 9 also contains a number of prohibitions which would seem at odds with section 5 and which would be unworkable in some areas of accepted UK practice. For example, in section 9.2 it is not clear how an official text would be capable of taking account of the complex landscape of 3rd parties that may or may not require access in a specific scenario. It is also worth noting that in the UK there is an active discussion on the appropriate balance of explicit consent or opt-out consent in important areas of public health such as cancer registries.

15.7. In section 9.3 this may need to be compared to the approach taken in the DH-BIO draft recommendation on predictive information and insurance. That recognises that in some situations, with consent, medical information can be shared with insurance companies in order to accurately assess the risk.

16.8. In section 12 we would strongly advise comparing the wording on consent and incapacity with the phrasing used in the Oviedo Convention and associated texts. It is important to distinguish between the consent of a person with capacity and the authorisation on behalf of a person – child or adult – without capacity. In section 12.2 there is a reference to genetic analysis which seems overly precise – we would argue that any diagnostic analysis should be within the objectives of the consultation and the scope of consent.

17.9. Section 13.6 is an example of overly complex drafting in an area that could have unintended effects. The effect of 13.6c(ii) could be such that an identical twin could prevent their sibling having access to important incidental findings that would be of direct importance to their health. There has been a case in the UK where a twin objected to her sister being tested for the BRCA mutations as she did not want to know her own status. Similar cases have been seen in Huntington's disease. It would be better in a recommendation to restrict this to 13.6a, b and the final sentence.

18.10. In editorial terms, all of Chapter IV reads more like a guide than a recommendation but has the advantage of not attempting to be overly prescriptive. It is also potentially more helpful to inform domestic policy and practice than an overly prescriptive drafting such as 13.6.

19.11. 18.3 Consent for research – the need for explicit consent for each defined research project is important but it would be helpful for this section to clarify the arrangements for research that are based on principles of anonymization or pseudo-anonymisation. A balanced approach to this would be consistent with the main data protection principles and with the concepts in section 4. From a quick search "anonymization" only appears in passing in the preamble.

20.12. We hope that these comments are helpful and that they can be incorporated into the recommendation to help ensure alignment with other Council of Europe texts and with the approach taken in countries such as the United Kingdom.

Greece

Hellenic Data Protection Authority

1. The definition of "health data" as any information of a biological and genetic nature (art.3) may be confusing with the following in the same article definition of "genetic data".

2. Given that the data subject should be informed for the explicit and specified purposes of the processing (art. 4.1.b.), the word "unambiguous" (art. 4.1.a.) should be replaced by "explicit" consent, in accordance to art.12.1.

3. According to greek law embryos who are not implanted in human body can not be subject of rights. Fetuses, on the other hand, are granted only an expectance of rights. What if there is a conflict of interest between parental rights and embryos/fetuses rights or embryos/fetuses rights and minors of the same family? (art. 6.1. and 6.2.)

4. In our opinion, prior to the exclusion established by art. 13.5.b. there should be given the chance to data subject to have access to his/her health data (i.e. mental health) through a health professional of his choice/trust.

5. In art. 15.4.e. it could be explicitly added as principle: enabling to monitor the processing of personal data by using log files.

Spain

1. General Overview

1. At first glance the Draft Recommendation seems to be a very comprehensive and complete legal tool, as it faces the new situations and questions that could arise from the health field and especially from biomedical research activities with an updated perspective. Indeed the provisions given are adequate for the future developments foreseen to ensure an efficient protection of health data, and especially of health related genetic data for the new challenges that health professionals will be confronted in the near future.

Accordingly with the previous considerations my personal evaluation of the Recommendation as a whole is very highly positive.

2. As I have highlighted above a strict and rigorous protection of genetic data should be met by the Recommendation as in short term the use of this kind of data will be more and more frequent in hospitals and in research labours. For this purpose the Additional Protocol concerning Genetic Testing for Health Purposes to the Human Rights and Biomedicine Council of Europe Convention (Oviedo Convention) is a crucial reference and legal tool in the European Legal System. The future Recommendation should be harmonized with the Additional Protocol and an explicit mention of it at the text of the Recommendation should be kept in mind (my personal suggestion would be to include its name at the text of the Recommendation as it has been taken into account).

2. Legally protected data

3. The Recommendation includes an adequate definition of "personal data" (principle 3). But it may occur that random (i.e., along a scientific research with anonymised health data) or after an intentional and unreasonable amount of time and effort data that have been previously anonymised could be back identified.

Although it is almost obvious, on legal security grounds the Recommendation should explicitly state that these data fall under the provisions of the Recommendation for personal data protection as they are again identified -or identifiable- data.

4. At the contrary I suggest also to the Committee to evaluate whether the following hypothesis should be considered as managing pseudonymised data and provide this consequently in the Recommendation. I am thinking on the possibility that an authorized and independent person of a concerned center (clinical hospital or biomedical research center) when he or she has exclusively the keys to re-identify codified personal data (pseudonymisation) that are used for a research team of that center. In this case that data should be considered as anonymised data (anonymous data) for all the members of the team if they have not access to the keys, as well as for third parties.

This would mean that such data didn't fall anymore under the provisions of the Recommendation as long as they remain codified for these persons and they have no means to identify such data. Only an authorized person to manage the keys data could be considered as managing pseudonymised data and would be applicable for him or her the provisions of the Recommendation (i.e., if it should be necessary to inform to the data subject on a recently diagnosed disease, when this disclosure had been agreed previously; on public health emergency grounds, etc.). This solution could facilitate to professionals (both clinicians and researchers) to manage these data more easily and communicate them (transfer) to other colleagues involved in the same or similar activity.

3. Big data and massive or whole gene sequencing

5. As a matter of checking the true efficiency of the Recommendation I think that the Consultative Committee (T-PD) should assess carefully whether the Recommendation has enough and specific provisions to respond to the new needs for data protection in relation with big data and massive or whole genes sequencing.

As it is generally known these kinds of data will give a very high number of personal information of a person being carrier of genetically related diseases, and this may be crucial on health and reproductive related decisions and a potential source for discrimination at a very relevant quality and quantity level. As a result the needs for a very qualified technical, management and legal protection are inalienable. Also the identification of the subject of such data derived from big data or massive genes sequencing is not excluded at all, even if they had been anonymized: crossing partial identified genetic data with that data (big data or massive or whole gene sequencing) even when they have been previously anonymized should be a relatively easy mean to re-identify such data.

In my view the Committee should pay attention to these weaknesses on the managing of genetic data in these cases and to prepare some adequate specific provisions to prevent these failing of protection of health data. Maybe banning crossing partially sequenced genetic identified data with that data after

its anonymization; but I am aware that a more accurately approach would be needed before to regulate this matter at the Recommendation.

4. Embryonic data

6. I agree completely with the provisions of the Recommendation addressed to protect health data of embryos and fetuses (principle 6). Otherwise the future newborns should be unprotected and in a weak position against discrimination as they were children or even adults.

In my view the wording "embryo" includes only the in utero embryo as it is placed in the Recommendation at the same level than the foetus, which necessarily is in pregnancy in the mother womb. But I think that this provision should cover the in vitro embryo as well, but only if it happens under a process of medically assisted reproduction, as in this situation it is frequent to do genetic tests to the embryo to discard that it is not carrier of a hereditary disease.

In my opinion the Recommendation should clarify that also health data of the in vitro embryo should be protected as this embryo has not still explicitly excluded for reproduction.

France

The draft recommendation covers the rights of persons (right to privacy, consent, user information), the use of sensitive health data for various purposes, the particularly tricky issue of restrictions on genetic testing (e.g. predictive medicine) and, lastly, research. However, these topics are covered by principles arising from the work of the DH-BIO to be found in: the Oviedo Convention, the Additional Protocols on biomedical research and genetic testing, the recommendation on research use of data associated with the collection of biological materials and the recommendation on genetic testing and insurance. They should accordingly be considered in the light of these texts in order to ensure overall consistency.

Generally speaking, this standard-setting document, although not legally binding since it is a recommendation, is not always as clearly drafted and legally precise as might be hoped (e.g. some passages are more explanatory statements than standard-setting provisions and the terms used are not sufficiently well-defined). The bioethics texts mentioned above should serve as references and could provide the missing definitions.

Introduction, page 3

- 4th §: some of the terms used are not sufficiently well-defined, which hinders understanding of their intended scope. For example, what should be understood by "mobility" [« *phénomènes de mobilité* »]: does this refer to issues related to the use of mobile telephones or more widely to aspects of telemedicine?

Similarly, does the reference to "connected medical objects and devices" [« *objets et dispositifs médicaux connectés* »] exclude non-medical objects? If so, what is the situation with regard to non-medical objects used for medical purposes?

Chapter I

- Purpose (p. 3): according to the draft recommendation the aim is to provide guidance on "processing and the different uses (of health data)" [« *l'utilisation et les différents usages* »]. These two similar terms should be defined more precisely by the T-PD if it considers that there

is a difference between them and that they apply to two different situations. This kind of precision is necessary to establish the scope of the recommendation.

Chapter II

- Section 4

The definition of consent and the different forms it takes are not clearly set out. Depending on the type of data or the purpose of processing (e.g. research, study, etc.), it may involve express, specific and documented consent or a right to object following notification. This point should be more closely linked with the principles set out in Chapter III regarding the right to information and consent.

Lastly, regarding point 4.4, it would be appropriate to clarify the role and responsibilities of the various actors. If data collection and processing can be entrusted to people who are not health professionals (technicians, epidemiologists, statisticians, etc.), there must be a guarantee that confidentiality and professional (or medical) secrecy will be respected in all cases.

- Section 5

How does this section link up with the principles set forth in section 4?

In general, it is very difficult to know when the recommendation applies to personal health data in the context of individual treatment or when the goal is "collective", i.e. for research or public health purposes.

It would therefore be preferable to clarify the overall presentation of section 5: for instance, are points 5.3 a), b) and c) cumulative?

- Section 6

On the issue of the embryo, see the comments regarding section 4.

The legal status of the foetus and embryo is not recognised in all the member States of the Council of Europe, in particular France. The European Court of Human Rights has laid down that "*it is neither desirable, nor even possible as matters stand, to answer in the abstract the question whether the unborn child is a person for the purposes of Article 2 of the Convention*" (ECHR, 8 July 2004, *Vo v. France*) and consequently allows member States full discretion in this regard.

In a Grand Chamber ruling of 27 August 2015, *Parillo v. Italy*, the Court took the view, in a case of donated embryos, that, since embryos contain the genetic makeup of the mother and thus constitute a part of her identity, she has a right to take action in defence of her right to respect for private life (as guaranteed by Article 8 of the Convention) and also that the member States had a wide margin of appreciation regarding the status of the embryo in the absence of any European consensus.[1]

In addition, point 6.2 states that the holder of parental responsibilities may act as the person legally entitled to represent the data subject. The concept "holder of parental responsibilities" [« détenteur des responsabilités parentales »] raises difficulties in respect of French domestic law and is not applicable

[1] Regarding this issue see also the observations on section 6 regarding the question of the embryo.

to the embryo or foetus. It consequently becomes necessary to refer to the “couple” from which the embryo originates.

Furthermore, if this section concerns preimplantation diagnosis (PID), it cannot relate to a foetus, since PID can only be made in vitro on an embryo. Once again, the embryo or foetus cannot be considered a (minor) person. These provisions could be incorporated in a different form under section 4 in order to specify what conditions apply to personal data collected before birth and processed later, in the case of the child or adult person.

- Section 7

Regarding **genetic data**, the draft recommendation does not draw a distinction between predictive and non-predictive data, and the methods of consent, which may differ, are never entered into in detail.

Regarding point 7.1: the interests of the data subject, of a related third person and of scientific research cannot be put on the same footing in respect of consent.

Point 7.2 is unclear, and the last sentence is difficult to interpret. Is the intention to refer to the problems bound up with the use of medical genetic data for non-medical purposes (e.g. for identifying a person in the legal context)? The differences between gene identification and pathological gene expression, and between coding and non-coding genes, could be discussed here.

What does point 7.3 cover? Which purposes other than those of a preventive, diagnostic or therapeutic nature? This point seems incomplete. Is use of data in the context of insurance or employment intended here?

Regarding point 7.4: the reference to the “social family” [« famille sociale »] has no meaning from the genetic standpoint, and what is meant by “consanguine or uterine relative” [« parent consanguin ou utérin »]? This expression needs to be clarified. More generally, what is the precise ambit of this paragraph?

- Section 8

Point 8.2 is not written in standard-setting terms, and it needs to be clarified what point 8.3 contributes in relation to point 8.2. The latter indeed limits what the former opens up.

- Section 9

Is the right to communication set out in full? Are some actors not omitted, such as research scientists? More details would permit clarification of the necessary guarantees.

- Section 10

This section would benefit from being more specific with regard to the change of purpose and point 10.3 falls more within the remit of chapter III.

Chapter III

- Section 11

This section deals with information in respect of the storage and processing of personal data. Point 11.3 therefore appears to be unclear insofar as it tackles the issue of the right to be kept in ignorance of a diagnosis, which itself arises from the right to information about health status within the doctor-patient relationship.

- Section 12

This section deals with consent and elicits remarks identical to those made in respect of the previous section: confusions have to be ironed out depending on whether data collection, storage or processing is intended.

The question of reporting results and consent to genetic testing is of a different order than consent to data processing. Collecting consent for “processing”, without specifying the purposes of this processing, seems vague. Is data collection, which is referred to in the previous section, also concerned by this section?

It follows that the methods for obtaining consent depending on circumstances (for example the purpose of research) and data types (predictive or non-predictive) ought to be defined more clearly.

Furthermore, it is not specified that consent must be obtained in writing, which nonetheless seems necessary in terms of evidence.

Lastly, the same sentence in point 12.3 covers a legally incapacitated person and a person who is incapable of free decision: are the two conditions cumulative?

Moreover, does this point refer solely to incapacitated adults or minors too? If this is the case, it should be indicated explicitly and there should be no reference to the capacity for free decision. Indeed, under French domestic law, a minor, even one capable of making decisions, is legally incompetent and must be represented.

- Section 13

Point 13.5 is not readily understandable and should be clarified. A distinction could be made between the purposes in order to avoid the accumulation of conditions and sub-conditions.

Point 13.6 concerns the rules on information to be laid down prior to genetic testing of a person within the framework of medical treatment and not of medical data processing.

Chapter IV

In the introduction to this chapter, aside from the fact that the two paragraphs do not contain standard-setting provisions, the second paragraph—which seems to indicate that the use of digital technology [« au numérique »] for better care is de facto “ethical” [« éthique »]—raises questions. In this regard, would it not be preferable simply to reiterate the need to adhere to the principles of necessity and proportionality or even to repeat the notion of balancing benefit/risk?

In addition, the draft recommendation should give a definition of what is meant by the expression “digital technology” [« au numérique »].

Chapter V

This chapter, which deals with research in the health field, could be redrafted by referring to the principles of the Oviedo Convention, the Additional Protocol on biomedical research and the recommendation on bio banks. It is an important chapter which should be clarified and further fleshed out.

Chapter VI

Like chapter V, this chapter seems in any case unfinished: it is not very precise and nor does it set standards but simply describes various situations.

EUROPEAN COMMISSION / COMMISSION EUROPEENNE

Recommendation CM/Rec(2016)…. of the Committee of Ministers to member States on the protection of health data

(adopted by the Committee of Ministers … 2016,

at the … meeting of the Ministers' Deputies)

States face major challenges today, relating to the processing of health data, which now takes place in an environment that has changed considerably since the adoption of Recommendation No. R (97)5 on the protection of medical data.

This changed environment is due to the phenomenon of data digitisation, made possible by the computerisation of the health sector and to the proliferation of exchanges arising from the development of the Internet.

Noteworthy features of this new environment are the growing computerisation of the professional sector and particularly of activities relating to care and prevention, to life sciences research and to health system management, and also the increasing involvement of patients.

Besides, mobility and the development of connected medical objects and devices contribute to new uses and to the production of a rapidly growing volume of data.

This assessment shared by the member States has prompted to propose a revision of Recommendation No. R (97) 5 on the protection of medical data, with the more general term "health data" being preferred, while reaffirming the sensitivity of health data and the importance of regulating their use so as to guarantee due regard for the rights and fundamental freedoms of the individual, in particular the right to privacy.

The Committee of Ministers, under the terms of Article 15.b of the Statute of the Council of Europe, recommends that the member States:

- ensure that the principles set forth in the appendix to the present Recommendation, which replaces Recommendation No. R (97) 5 mentioned above, are reflected in the implementation of national legislation on protection of health data, as well as in other branches of any law on the use of health data;
- ensure, to that end, that the present Recommendation and its appendix are brought to the attention of the authorities set up under national data protection legislation to monitor the application of that legislation, as well as of the authorities responsible for healthcare systems;
- promote acceptance and application of the principles set forth in the appendix to the present Recommendation, using additional instruments such as codes of conduct, while ensuring that these principles are well-known, understood and applied by all the players in the healthcare sector and taken into account in the design, deployment and use of the ICTs in that sector.

Appendix to Recommendation CM/Rec(2016)…

Chapter I

General provisions

5. Purpose

The purpose of this Recommendation is to provide member States with guidance for regulating the processing, and the different uses, of health data in order to guarantee respect for the rights and fundamental freedoms of every natural person, particularly the right to privacy. It also provides guidelines for developing interoperable and secured information systems in a manner enabling the quality of care and the efficiency of health systems to be enhanced.

6. Scope

This Recommendation is applicable to the processing of personal data relating to health (health data) in the public and private sectors.

It also lays down the principles for the exchange and sharing of health data by means of digital tools with due regard for the rights of the individual and the confidentiality of data.

The provisions of this Recommendation do not apply to health data processing performed by individuals in the context of exclusively personal or domestic activities.

7. Definitions

For the purposes of this Recommendation, the following expressions are defined as follows:

- The expression “personal data” refers to any information relating to an identified or identifiable individual. An individual shall not be regarded as “identifiable” if identification requires an unreasonable amount of time, costs and effort taking into account the available technology at the time of the processing and technological developments. In cases where the individual is not identifiable, the data are referred to as anonymous.

- The term "controller" means the natural or legal person, public authority, service, agency, or any other body which, alone or jointly with others, has the decision-making power with respect to data processing;

- The term "processor" means a natural person or legal person, public authority, service, agency, or any other body to whom data are disclosed or made available;

- ~~The expression~~ “health data” covers all data that may reveal the data subject’s ~~past, present or future~~ state of health in relation to his/her physical and/or mental condition~~, irrespective of their source~~. It also covers any information relating to ~~his/her~~ the ~~health and welfare~~ provision of healthcare services which reveals information about his or her state of health. It may also involve information of a biological and genetic nature. It further covers data relating to well-being and/or lifestyle where these reveal a state of health.

- The expression “genetic data” refers to any data relating to an individual's genetic characteristics, whether inherited or acquired at an early stage of prenatal development, which give unique information about the physiology or the health of a natural person resulting from the analysis of a biological sample from that individual: analysis of chromosomes, DNA or RNA or any other component making it possible to obtain equivalent information.

- The expression "reference framework" denotes a coordinated set of rules and/or processes kept constantly state-of-the-art and applicable to health information systems, covering the areas of identification, interoperability and security.

- The expression "electronic medical file" denotes a secured set of health data, structured or not, of one individual, which accompanies them throughout the course of their treatment. It enables the patient and authorised health professionals to share the information that is useful for co-ordinating care.

- The expression "secure messaging system" denotes a service for the secure exchange of personal health data between identified individuals.

- The expression "right to portability" denotes a person's right to receive data concerning them that have been entrusted to a data controller, where the processing is based on the consent of the data subject or on a contract, in a structured, commonly used format, and to transmit them, if necessary, to another controller.

- The expression "mobile applications" denotes a set of means accessible in a mobile environment making it possible to communicate and manage health data remotely. It covers different forms such as connected medical objects and devices.

- The expression “health professionals” covers all professionals recognised as such by national and European Union law practising in the health, medical welfare or social welfare sector, bound by professional secrecy and involved in co-ordinating treatment for an individual to whom they provide health care.

- The expression "health data hosting" denotes the use of data storage service provider ~~third-party agencies~~ for the secure and lasting storage of health data by analogical or digital means~~on the Internet~~.

- The expression "anonymisation" denotes the process applied to health data so that the data subject can no longer be identified, either directly or indirectly. ~~Anonymisation is irreversible~~.

- The expression "pseudonymisation" ~~denotes~~ a technique whereby data can be made non-identifying for as long as they are not associated with other elements stored separately which would make identification possible. Pseudonymised data are personal data.

- The concepts of exchange and sharing of health data, which can be features of health data processing, are defined as follows:

(a) Data exchange is the communication of information to a clearly identified recipient or recipients by a known transmitting party.

(b) Data sharing enables data to be made available to several persons entitled to be made aware of such data according to the principles of the right of access, without these persons necessarily being known at the outset.

- The term communication refers to any processing operation and in particular the exchange or sharing of personal data enabling authorised persons to have access to personal data, regardless of the means or devices used.

Chapter II

The legal conditions for use of health data

~~8. *Privacy by design*~~

4.1 Anyone processing health data should~~must~~ comply with the following principles:

~~w.~~cc. The processing of data should be proportionate in relation to the legitimate purpose pursued and shall be carried out only on the basis of free, specific, informed and unambiguous consent of the data subject or on other legitimate basis laid down by law.

~~x.~~dd. Personal data must be processed lawfully and fairly. They must be collected for explicit, specified and legitimate purposes and must not be further processed in a manner that is incompatible with these purposes; ~~subsequent~~ further processing for~~-~~ archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is compatible with those purposes on condition that additional guarantees apply.

~~y.~~ee. The data must be adequate, relevant and not excessive in view of the purposes for which they are processed; they must be accurate and, if necessary, updated.

~~z.~~ff. The data must be stored in a form allowing identification of the data subjects for a period not beyond what is necessary for the purposes for which they are processed.

~~aa.~~gg. Appropriate security measures ~~must~~should be established to prevent risks such as accidental or unauthorised access to personal data or the destruction, loss, use, modification or disclosure to unauthorised third parties of those data.

~~bb.~~hh. The rights of the person whose data are collected and processed must be respected, particularly their rights of access to the data, information~~communication~~, rectification, ~~and~~ objection and erasure.

4.2 The processing of health data is permissible only insofar as ~~specific and~~ appropriate guarantees are provided for by ~~in~~ ~~domestic~~ law complementing those of Convention 108 to prevent any risk to the interests, rights and fundamental freedoms of the data subject which the processing may represent, in particular the risk of discrimination.

4.3 The purposes for which health data are processed must also be taken into account in order to ensure appropriate use of these data and to adapt the safeguards accordingly.

Comment [A193]: Privacy by design does not qualify as a legal condition to use data. It is rather a technique to implement data protection principles.

Comment [A194]: First requirement is that data are processed lawfully (point b). consider reverting these two points/.

4.4 In principle, health data ~~must~~should be collected and processed by health professionals, agencies acting under the responsibility of health professionals or by the data subjects themselves. Data controllers and their processors who are not health professionals should ~~only~~ collect and process health data in accordance with the same rules of confidentiality and security measures that apply to health professionals.

Comment [A195]: "Only" seem to be unduly restrictive.

Comment [A196]: The formulation of this requirement suggests that this requirement is an additional one to the processing of health data. This is not justified neither under GDPR or Convention 108.

4.5 These personal data protection principles must be taken into account and incorporated right from the design of information systems collecting and processing~~, using and exploiting~~ health data. Compliance with these principles ~~must~~should be regularly reviewed throughout the life cycle of the processing. The controller ~~must~~should assess the impact of the applications used in terms of data protection and respect for privacy.

4.6 The controller ~~must~~should take all appropriate measures to fulfil their obligations with regard to data protection and ~~must~~should be able to demonstrate in particular to the competent supervisory authority that the processing for which they are responsible is in line with those obligations.

5. Processing of health data

5.1 Health data must be processed fairly and lawfully and only for specified purposes.

Comment [A197]: Repetition with point 4.1.b above

~~5.2 Health data shall in principle be collected from the data subject. They may be collected from other sources only if in accordance with principles 5, 6, 7, 9 and 12 of this Recommendation and if this is necessary to achieve the purpose of the processing or if the data subject is not in a position to provide the data.~~

Comment [A198]: This is too restrictive. Under GDPR and the Convention 108 health data collected from different soruces.

5.3 Health data may be processed ~~and communicated~~:

~~j. if provided for by law or if the processing is based on a contract concluded with a health professional stipulating appropriate safeguards;~~

~~xiii. for preventive medical purposes and for purposes of medical diagnoses, administration of care or treatment, or management of health services by health professionals and those of the social and medical welfare sector;~~

~~xiv. for reasons of public interest in the public health field, such as for example protection against international health hazards or in order to ensure a high standard of quality and safety for medical treatment, health products and medical devices;~~

~~xv. for reasons of public interest in the field of managing claims for social welfare and health insurance benefits and services;~~

~~xvi. for reasons of public health provided they are lawful, legitimate and compatible with the initial purpose of the data collection;~~

Comment [A199]: Under Convention 108 processing for health data is not possible on the basis of a contract. Besides, all the points refer to processing for public interest reason and it is difficult to imagine how they could be based on a contract.

~~k.~~m. if the data subject has given his or her consent in accordance with principle 12 of this Recommendation, except in cases where domestic law provides that a ban on processing health data cannot be lifted solely by the data subject's consent;

~~l.~~n. insofar as it is authorised by law, in particular:

~~xvi.~~xxi. for purposes of safeguarding the vital interests of the data subject or of a person physically or legally incapable of expressing consent;

~~xvii.~~xxii. for reasons relating to the obligations of the controllers and to the exercise of their rights or those of the data subject regarding employment and social protection, in accordance with domestic legislation or any collective agreement complying with the said legislation and providing for appropriate safeguards;

~~xviii.~~xxiii. for reasons essential to the recognition, exercise or defence of a legal claim;

~~xix.~~xxiv. for reasons relating to research in the field of health and the medical welfare sector;

for processing for archiving purposes in the public interest, for statistical, historical or scientific research purposes on the basis of ~~under the conditions defined by~~ domestic law, which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable measures to safeguard the fundamental rights and the interests of the data subject. ~~to guarantee protection of the data subject's legitimate interests and where the individual cannot be identified~~

~~xx. from the results.~~

In all cases, suitable guarantees ~~must~~should be established to ensure in particular the security of data and respect for the rights of the individual. Any other guarantees may be provided for in domestic law with a view to safeguarding respect for rights and fundamental freedoms.

6. Data concerning embryos and foetuses

6.1 Medical data concerning embryos and foetuses, *inter alia* such as data resulting from a pre-implantation diagnosis, should be considered as personal data and enjoy protection comparable to the protection of the health data of a minor.

6.2 Unless otherwise provided for by domestic law, the holder of parental responsibilities may act as the person legally entitled to act in the capacity of data subject.

7. Genetic data

7.1 Genetic data processed with a preventive aim, for diagnosis or for treatment of the data subject or a third person (genetic testing on a legally incapacitated person for the benefit of family members for example) or for scientific research should be used only for th~~o~~ose purposes or to enable the data subject to take a free and informed decision on th~~o~~ose matters.

7.2 Processing of genetic data for the purpose of a judicial procedure or a criminal investigation should be the subject of a specific law offering appropriate safeguards. Such law might provide that ~~The~~ data might ~~should~~ be used ~~only~~ notably to establish whether there is a genetic link in the context of the production of evidence, to prevent a real danger or to punish a specific criminal offence. In no case should they be used to determine other characteristics which may be linked genetically.

7.3 Any processing of genetic data other than in the cases provided for in paragraphs 7.1 and 7.2 should be authorised by the law, particularly where carried out to avoid any serious prejudice to the health of the data subject or third parties. Genetic data may not be used for commercial exploitation in any circumstances. The processing of genetic data in order to predict illness may be authorised in the vital interest and subject to appropriate safeguards provided for by law.

7.4 The publication of genetic data which would identify the data subject, a consanguine or uterine relative of the data subject, a member of his/her social family or a person who has a direct link with his/her genetic line, should, in principle, ~~-~~be prohibited.

Formatted: Indent: Left: 0 cm

Formatted: Indent: Left: 0 cm

Comment [A200]: . A wider use of data may be provided by the legislator. In any event the paragraph addresses an issue that goes far beyond the processing of data and would be better deleted.

Comment [A201]: This expression is too broad and open for interpretation. It must be possible to use genetic data for research in areas such as population genomics and genetics of complex traits. Commercial exploitation of genetic data e.g. for insurance purposes should be prohibited, but we do not want to prohibit commercial exploitation based on genetic data for the development of genetic diagnostics or new therapies. In any event the paragraph addresses an issue that goes far beyond the processing of data and would be better deleted.

Comment [A202]: This is too restrictive. Processing of genetic data to predict illness should be possible based on consent as well, and for public health purposes where defined in an appropriate legal instrument.

Comment [A203]: The conditions for using genetic data mentioned in the text are not warranted by Convention 108 and are also stricter and therefore incompatible with the GDPR.

Comment [A204]: Genetic data poses the risk of re-identification. The proposed general prohibition of publication of (potentially identifiable) genetic data is too restrictive. Publication of genetic data should be allowed based on consent or the law notably where it is necessary to present research findings.

8. Shared medical secrecy for purposes of providing and administering care

8.1 Everyone is entitled to protection of his or her health data. The person receiving care is entitled to respect for his or her privacy and the secrecy of the information concerning them in dealings with a professional operating in the health, medical welfare and social sector.

8.2 In the interests of greater co-ordination between professionals operating in the health and social and medical welfare sector, the domestic law of each member State should recognise a shared professional secrecy, between professionals who are themselves legally bound by such secrecy.

8.3 The exchange and sharing of data between health professionals ~~must~~should be limited to the information strictly necessary for the co-ordination or continuity of care, prevention or medical welfare-related and social monitoring of the individual, with the respective actors only able to pass on or receive data lying strictly within the scope of their tasks.

Comment [A205]: This is too restrictive in particular where health data are collected from sources other than the individual and processed in the public interest (e.g. for reasons of public health)

8.4 The data subject ~~must~~should be informed beforehand of the nature of the data collected and processed and of the health professionals participating in the care team and must be able to object at any time to the exchange and sharing of his or her health data.

9. Communication to authorised third parties

9.1 Health data should ~~must~~ not be communicated, except in the conditions set out in this Recommendation.

9.2 They may be communicated to third parties where the latter are authorised by domestic law to have ~~ad hoc and limited~~ access to the data. These third parties may notably be judicial authorities, experts appointed by a court authority or members of staff of an administrative authority designated by an official text.

9.3 Medical officers of insurance companies and employers cannot be regarded as third parties authorised to have access to the health data of patients.

10. Storage of health data

10.1 Health data should be stored only for the time necessary to achieve the purposes for which they were collected. Domestic law may provide for exact storage periods having regard to the nature of the health data storage medium.

10.2 Storage of health data for other purposes than those for which they were initially collected ~~must~~should be carried out in compliance with the principles of this Recommendation.

10.3 The data subject may personally request deletion of his/her data unless they have been ~~irreversibly~~ rendered anonymous or legitimate interests preclude this.

Chapter III

The rights of the individual

11. Right to information

11.1 Everyone must be informed of the collection and processing of their health data.

They must be informed of:

- the identity and contact details of the controller and of the processors where relevant,
- the purpose for which the data are processed, and where appropriate of the relevant legal basis for it,
- how long the data will be stored or if that is not possible, the criteria used to determine that period;,
- the recipients or categories of recipients of the data, and planned data transfers to a third country or international organisation,
- where applicable, the possibility to object to ~~of refusing~~ the processing of their data, or of withdrawing their initial consent~~, and the implications of such withdrawal~~,
- the possibility of their data being subsequently processed for a compatible purpose, in accordance with appropriate safeguards provided for by domestic law,
- ~~the specific techniques used for processing their health data,~~
- the conditions and the means made available to them for exercising via the controller their rights of access, the right of rectification and deletion of their health data, and the possibility to object to the processing thereof.
- the possibility to lodge a complaint with a supervisory authority
- the existence of automated decision-making including profiling.

11.2 This information should be provided at the time of data collection or of the first communication.~~,~~ Where the data relating to a data subject is obtained from the data subject this requirement should not apply ~~unless~~where and insofar as the data subject already has the information.

Where the data relating to a data subject has not been obtained from the data subject, the above information should be provided at the time of data collection or of the first communication, unless

- it proves impossible or requires disproportionate efforts, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes or in so far as the obligation to provide information is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller should take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;
- obtaining or disclosure is expressly laid down in domestic law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests;
- where the personal data must remain confidential subject to an obligation of professional secrecy regulated by law, including a statutory obligation of secrecy;

The information ~~. It~~ must be appropriate and suited to the circumstances. In particular, where the data subject is physically or legally incapable of receiving the information, it may be given to the person legally representing him/her. If a legally incapacitated person is capable of understanding, he/she should be informed before his/her data are processed.

Formatted: English (U.K.)

Formatted: Bulleted + Level: 1 + Aligned at: 0,74 cm + Indent at: 1,37 cm

Formatted: English (U.S.)

Formatted: English (U.S.)

Formatted: English (U.S.)

Formatted: English (U.S.)

11.3 Information provided to the data subject may be restricted if such derogation is provided for by law and constitutes a necessary and proportionate measure in a democratic society:

- to prevent a real danger ~~or to punish a criminal offence,~~
- for public health reasons,
- to protect the subject and the rights and freedoms of others;
- for the protection of national security, defence, public safety, important economic and financial interests of the State, the impartiality and independence of the judiciary or the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties, and other essential objectives of general public interest;
- historical research purposes or statistical purposes where there is no identifiable risk of an infringement of the rights and fundamental freedoms of data subjects, in particular where such data are not used for decisions or measures relating to a specific individual.
- .

Formatted: Normal, No bullets or numbering

Formatted: Normal, No bullets or numbering

Formatted: Normal, No bullets or numbering

11.4 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. In a medical emergency, when the person's life is at stake, care takes precedence over information.

11.5 Domestic law ~~must~~should provide for appropriate safeguards ensuring respect for these rights.

12. Consent

12.1 Where the data subject is required to give his/her consent to the processing of health data, this consent should be free, specific, informed and explicit. When the consent is given digitally, it should be tracked. It does not discharges ~~absolve~~ the person receiving it of the obligations to give prior information.

Comment [A206]: Unclear. Does it refer to an obligation of keeping a record?

12.2 The processing ~~results~~ of genetic data for analyses purposes ~~analyses~~ should stay ~~be formulated~~ within the limits of the objectives of the medical consultation, diagnosis or treatment for which consent was obtained.

~~12.3 Where it is intended to process health data relating to a legally incapacitated person who is incapable of free decision, and where domestic law does not authorise the data subject to act on his/her own behalf, consent is required from the person recognised as legally entitled to act in the interest of the data subject or from an authority or any person or body provided for by law.~~

~~12.4 If a legally incapacitated person has been informed of the intention to process his/her health data, his/her wishes should be taken into account, unless domestic law provides otherwise.~~

Comment [A207]: Deleted paragraphs concern matters of State civil law. We wonder if it should be included in a recommendation on data protection. This comment applies to all subsequent deletions of similar paragraphs on this subject.

13. **Right of access, objection, rectification, erasure and portability**

13.1 Everyone should have right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information

- **the purposes of the processing;**
- **the categories of personal data concerned;**
- **the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;**
- **where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;**
- **the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;**
- **the right to lodge a complaint with a supervisory authority;**
- **where the personal data are not collected from the data subject, any available information as to their source;**
- **the existence of automated decision-making, including profiling.**
- ~~**must be able to secure access to his or her health data directly from whoever holds them.**~~

Formatted: Bulleted + Level: 1 + Aligned at: 0,63 cm + Indent at: 1,27 cm

13.2 The right of access, implying the right to communication of information, on paper as well, enables the data subject to exercise his/her right of rectification and deletion. It also encompasses the right to receive data in a structured format, where the processing is based on consent or on a contract, and is carried out by automated means, making it possible to transmit them to another controller designated by the data subject.

13.3 The right of erasure ~~deletion~~ is exercised subject to the cases prescribed by ~~domestic~~ law invoking legitimate grounds.

The data subject is entitled to object on ~~legitimate~~ grounds related to his or her situation to the collection of his/her personal health data except where the person holding the data invokes an overriding and legitimate reason concerning the public interest of public health.

13.4 If the request to rectify or erase ~~delete~~ the data is refused or if the data subject's objection is rejected, he or she ~~must~~should be able to appeal.

Comment [A208]: Right of rectification has not been mentioned before.

13.5 Access to health data may be refused, limited or delayed only if the law provides for it and if:

~~e.~~i. this constitutes a necessary and appropriate measure in a democratic society in the interests of protecting defence, national security or public safety, or of preventing, investigating or punishing criminal offences~~, or~~ and the execution of criminal penalties, and other essential objectives of general public interest;

Formatted: Normal

~~f.~~j. knowledge of the information is likely to cause serious harm to the data subject's health; or

Comment [A209]: Who takes the decision in such cases?

~~g.~~k. the information on the data subject also reveals information on third parties or if, with respect to genetic data, this information is likely to cause serious harm to a consanguine or uterine relative or to a person who has a direct link with this genetic line; or

l. ~~the data are used for~~ archiving purposes in the public interest, scientific or historical research purposes or statistical purposes where there is no identifiable risk of an

Formatted: Normal

infringement of the rights and fundamental freedoms of data subjects~~, in particular where such data are not used for decisions or measures relating to a specific individual.~~

~~h.~~m.

13.6 The person subjected to genetic analysis should be informed of unexpected findings if the following conditions are met:

d. domestic law does not prohibit the provision of such information;

e. the person himself or herself has asked for this information;

f. the information is not likely to cause serious harm;

iii. to his/her health; or

iv. to a consanguine or uterine relative, to a member of his/her social family, or to a person who has a direct link with his/her genetic line, unless domestic law provides other appropriate safeguards:

Subject to domestic law, the person should also be informed if this information is of direct importance to him/her for treatment or prevention.

Comment [A210]: Although the CoE Recommendation No. R (97) 5 from February 13, 1997 includes the same provisions the question is whether this is the right place for giving recommendations on the reporting of unexpected (or incidental or unsolicited) findings of genetic tests which is subject of a continuous debate among clinical geneticists. The current text misses the importance of genetic counselling in the process.

Chapter IV

Reference frameworks for the processing of health data

In the processing of health data all players ~~must~~should observe high standards to ensure the confidentiality of particularly important ~~sensitive~~ health data. The possible uses of these data and their disclosure, whether voluntary or not, are potentially highly damaging to an individual. But the issues of data availability (when a critical medical act is to be carried out, for example), integrity and auditability (including traceability) are equally vital.

Comment [A211]: Only the paragraphs that might be related and useful to data protection should remain. All the rest should be deleted.

Comment [A212]: In this chapter there are fragments which are not data protection related and we suggest to delete them (see in tc below)

~~As the use of digital technology leads to better care, technical considerations take on an ethical dimension, with data availability and interoperability converging with the notion of continuity of care and equality, and technical irreversibility potentially resulting in a loss of opportunity for patients for example.~~

14. Reference frameworks

~~14.1 In accordance with the principle of privacy by design as defined in paragraph 4.5,~~ the applications which manage health data ~~must~~should, from their design onwards, incorporate the principles of data protection and the relevant security and ~~interoperability~~ reference frameworks and ensure that the processing of the data complies with these principles and reference frameworks.

~~14.2 The aim of these reference frameworks is, depending on the use made of data, to define in co-ordination with all the players the conditions governing the use of health data in information systems with a view to ensuring their confidentiality and interoperability. They cover the areas of identification, interoperability and security.~~

~~g)~~

Formatted: No bullets or numbering

16. Security reference frameworks

16.1 The processing of health data ~~must~~should be secure ~~and use solutions guaranteeing the availability, integrity, confidentiality and auditability of data~~.

16.2 These security rules, kept constantly state-of-the-art, should result in the adoption of such technical and organisational measures as to protect personal health data from any illegal or accidental destruction, any loss or any impairment, and to guard against any unauthorised access. In particular, domestic law ~~must~~should make provision for organising and regulating health data collection, storage and restitution procedures.

16.3 System availability– i.e. the proper functioning of the system – ~~must~~should be ensured by measures enabling the data to be made accessible in a secure way and with due regard for each person's permissions.

~~1~~6.4 Guaranteeing integrity requires verification of every action carried out on the nature of the data, any changes made to or deletion of data, including the communication of data. It also

1~~6.5 Data confidentiality~~ requires the establishment of measures to monitor access to the data servers and the data themselves, ensuring that only authorised persons are able to access the data.

16.6 Auditability means that there ~~must~~should be a system making it possible to trace any access to the information system and for any action carried out by an individual to be logged to that individual.

16.7 Activity entailing storing health data in analogue and digital systems ~~on the Internet~~ and making them available for users ~~must~~should comply with the security reference framework and principles of personal data protection.

16.8 Professionals who are not directly involved in the person's health care, but by virtue of their assigned tasks ensure the smooth operation of the information systems, may have access, insofar as this is necessary for the fulfilment of their duties and on an ad hoc basis, to personal health data. They ~~must~~should have full regard for professional secrecy and with appropriate measures laid down in domestic law to guarantee the confidentiality and security of the data.

~~**17. Health data management services**~~

~~17.1 Each member state should establish services for the exchange and sharing of health data as useful aids especially for the co-ordination of care, complying with security and interoperability reference framework defined in sections 14 to 16.~~

~~**Since these capabilities for exchange and sharing contribute to the quality of care provision and to the proper management of health systems as well as to other goals, for the benefit of both individuals and the collective interest and public health, professionals in the health and**~~

~~**social and medical welfare sector should each be equipped for the electronic management of their activity, enabling them to exchange or share personal health data.**~~

~~17.2 Patients must have the benefit of a secure electronic medical file enabling them to have information useful to their medical, welfare and social monitoring throughout their course of treatment.~~

~~The information in this medical file may be shared, with the patient's consent, by professionals involved in care provision for the patient in the conditions defined in paragraph 8.1.~~

~~17.3 Any electronic messaging system permitting the exchange of personal health data must comply with the reference framework defined in section 14.~~

Chapter V - Research in the health field

18. **Research in the health field**

18.1 The use of health data for the purposes of research in the health field ~~must~~should be carried out with a legitimate aim and in full compliance with the principles laid down in this Recommendation.

18.2 The need to use health data ~~must~~should be evaluated in the light of the aim pursued.

18.3 Persons whose data are being used for research ~~must~~should be informed, where applicable, of such use and, where provided for by ~~in domestic~~ law, give their consent, except in cases of medical emergency.

~~When the data subject is a legally incapacitated person and domestic law does not authorise the data subject to act on his/her own behalf, his/her legal representative or an authority, or any person or body provided for by law, shall~~should ~~be provided with the information and/or shall~~should ~~give his or her consent in the context of the research project.~~

~~18.4 The conditions in which health data are processed for research in the health field and, in particular, the value of such data for public health must be assessed by the body or bodies designated by domestic law;~~

~~18.5 Subject to additional provisions determined by domestic law, health-care professionals entitled to carry out their own medical research should be able to use the health data which they hold as long as the data subject has been informed of this possibility and has not objected.~~

18.6 Personal data used for scientific research may not be published in a form which enables the data subjects to be identified, unless they have given their consent for the publication or ~~and~~ publication is authorised by ~~domestic~~ law.

In all cases appropriate safeguards ~~must~~should be introduced to ensure in particular data security and respect for the rights of the individual. Any other guarantees may be provided for in domestic law with a view to safeguarding respect for human rights and fundamental freedoms.

Comment [A213]: Doubling. confusion; "research purpose" is an aim. Unclear what is meant by this sentence. Three concepts seem to be used for the same reality: purpose; aim and use. Need to be consistent in terminilogy.

Comment [A214]: According to GDPR processing of sensitive data for scientific research should be subject to one of the conditions provided for in Art. 9 (2) and in particular point (j).
However, the Convention 108 only requires appropriate safeguards which shall be complementary to the ones established under the Convention.

Comment [A215]: Deleted paragraph does not add value and is in any case of comptenete of Member Sattes.

Comment [A216]: We are not sure that this paragraph has any added value. If it should be understood as permitting the use of data for research purposes without being authorised by law and on the basis of a simple opt-out clause, this would not be compliant with the modernised Convention 108

Chapter VI – Mobile applications

19. Mobile applications

19.1 The development of mobile applications enables both patients and professionals in the health sector and the welfare and social sector to collect health data and process them remotely. This development takes on different forms and covers several categories of applications, themselves pursuing very different goals of use. Ranging from medical applications to "quantified self" applications, connected devices make it possible to quantify and/or evaluate parameters that may reveal a person's state of health and, in certain cases, are used directly to make diagnoses and provide care.

19.2 Where the data collected by these applications may reveal a person's state of health, concern any information regarding their health care and welfare provision and/or are processed in a medical context, they constitute health data. In this connection they ~~must~~should enjoy the same legal protection and confidentiality applicable to other methods of health data processing as defined by the present Recommendation and, where applicable, supplemented by the domestic law of States.

19.3 Well-being or self-measurement applications used solely for the benefit of the individual using them, operated for solely personal reasons and not generating any external communication should not be considered as being subject to the requirements of the present Recommendation. Guidance on the application of data protection principles to the processing of health data by private sector entities in the context of the use of mobile applications is to be provided distinctly from the present Recommendation.

INTERNATIONAL CHAMBER OF COMMERCE (ICC) / CHAMBRE INTERNATIONALE DU COMMERCE (CIC)

The International Chamber of Commerce (ICC) is the world business organization and works to further the development of an open world economy with the firm conviction that international commercial exchanges are conducive to both greater global prosperity and peace among nations. Consisting of over six million companies, chambers of commerce and business associations in more than 130 countries ICC has vast experience providing business expertise to policy-makers globally.

ICC's Commission on the Digital Economy develops policy positions and practical tools for the Internet and information communications technology (ICTs). The Council of Europe "*Draft recommendation on the protection of health data"* provides principles for the exchange and sharing of health data by means of digital tools and raises important factors which would benefit from cross-sectoral business experience and expertise. Through these comments ICC would like to highlight the societal benefits of emerging technology and share perspectives on the importance of balanced, flexible, multistakeholder approaches to managing the privacy and security implications of their use.

The Council of Europe is both justified and timely in developing guidance related to health data. Data is used and exchanged at ever-increasing levels and data flows are increasingly being recognized as catalyzing economic efficiency and productivity, raising welfare and standards of living. Preventative healthcare offers immense opportunities for health-care providers and systems by predicting disease, developing treatments, providing greater efficiency and freeing up scarce resources, for the treatment and benefit of patients. Carefully balancing opportunities to realize the benefits of technology for health-systems and ensuring effective security, privacy and confidentiality of personally identifiable patient information is therefore of increasing importance.

ICC would like to highlight a question that the Council of Europe has arguably missed which underscores an important factor to reflect on when considering the use of technology for societal benefit particularly with regard to health: How can professionals use and further innovate their use of technologies and practices in ways that benefit society while ensuring the effective security, privacy and confidentiality of personally identifiable information?

While Chapter IV of the Council of Europe recommendation makes reference to beneficial uses of data, ICC suggests including an explicit statement highlighting the importance of applying technology and safeguarding privacy in the sharing and use of health and medical data for societal benefit. Health is arguably as much of a fundamental right as privacy and the possible "lost opportunity" in health care if technology is not applied or innovated may have fatal consequences for patients and future generations. Health and privacy are too often seen as competing concepts which does not have to be the case. Indeed similarly to other sectors, there are many opportunities to optimize health systems across innovative use of data and ensure the protection of personal data and health care rights.

The Council Europe correctly identifies the use and benefit of electronic medical records as well as the growing importance of medical applications and those applications which may track data potentially related to medical data; fitness "wearables" etc. ICC underscores that it is challenging to provide guidance for an emerging set of products, as their role and use can be unclear. For example, in Seattle a team of orthopedic surgeons started sending patients home with a gaming console because of its ability to track motion which allowed patients to evaluate their range of motion in physical therapy. A gaming console would arguably not be considered a medical device, but the innovative use of non-medical technology, allowed the practice to optimize patient visits assuring that those making good progress could continue at home and those not progressing could be called into the surgery. The use of technology resulted in fewer patient visits, greater patient satisfaction, better patient outcomes and cost savings to both the practice and insurance.

The importance of flexibly is especially true for emerging technologies such as cloud, big data and the Internet of things. While these concepts are well known, current uses are only beginning to understand and exploit their true potential. According to McKenzie such emerging technologies will have a profound economic impact of $3.9 trillion to $11.1 trillion a year by 20251.

[1] http://www.mckinsey.com/insights/business_technology/the_internet_of_things_the_value_of_digitizing_the_physical_world

***

The Council of Europe is drafting guidance related to big data and we reference the ICC comments on same. Big data models are predicated on the ability to associate streams of data from varied and often fast changing, real-time sources. Associated correlations across data may yield insights that lead researchers to ask new questions of potential significance. For example, in the case of health this could lead to new treatments of disease. Those correlations give rise to the potential purpose for which the data may be beneficially used and may fuel the following questions: How can one provide a specific and explicit consent when the use of information may not be known? Do we forgo the potential benefits of innovation? Is the missed innovation that would benefit a fundamental right (for example health) transferred into an opportunity cost to society?

The Council of Europe recommendation contains inferences which can be expanded into a possible solution path. Section 4.1b introduces the concept of compatible processing for historical, scientific and statistical purposes “on condition that additional guarantees apply”. Section 18.5 includes the possibility of practitioners using collected medical health data for unspecified compatible future research as long as the data subject has been informed of, and not objected to, the possibility. These could become the building blocks for a more flexible approach. Additional guarantees could be developed to assure that appropriate and validated security and privacy protocols are in place with appropriate sharing limitations. This may permit the use of more generalized purpose specifications with flexibility for future innovative use while enabling data subjects such as patients to feel confident about the circumstances of the processing. Similarly where previously information was collected with only a specific and limited consent, more compatible uses of information for research purposes may be found where the lack of new individualized consent is replaced by appropriate ethical review. This review would be compliant with established research norms in the relevant sector such as a health, and consider appropriate stakeholder interests and expertise.

While the Council of Europe recommendation may not specifically preclude such explorations, the opportunity to enter into constructive discussions of what such a framework might look like and what it could accomplish should be encouraged. Furthermore, a risk particularly penitent to the health community related to privacy is developing where researchers are limiting their scope of innovation from a fear of privacy transgression or overwhelming administrative burden. ICC encourages a dialog that results in both enhanced innovation and privacy.

ICC would also like to raise a couple of drafting concerns:

Definitions:

Reference framework: The reference to “state of the art” needs to be qualified to be adaptable to context. Context includes the nature of the data, the nature of the processing and the nature of the entity. The technology should be up to date and using practices appropriate to the nature and circumstances of the data and the processing entity.

Electronic medical file: This may often exist beyond as course of treatment as the medical record of the patient and should be revised accordingly.

Data portability: The use of the term “receive” indicates that data will always be sent, in some cases it will be made accessible rather than sent due to the nature of the information. Preferred word would be the right to “obtain”.

Health data hosting: “Lasting” makes one think of an archive, hosting may not be so permanent.
Anonymization/ pseudonymization: Consider using a broader term of de-identification as a chapeau which would include both terms but not be limited to them. Allows for future innovation, also

de-identification lends itself more to a contextual analysis – de-identified to the extent appropriate for the nature of the data and its intended use.

7.3 – banning commercial exploitation: The limitations on commercial use are overbroad. As written, genetic information may be precluded in pharmaceutical research or trials that lead to commercial products. The limitation should be more narrowly drafted.

9.2: Takes a very limited view of the nature and scope of third parties and does not include sharing that is consented to by the patient or pursuant to a health care agreement that may provide ongoing access to health data.

10.1 – stored for the period of time they were collected or during which it was agreed or possible for which they could be used: Purpose of collection may not include all compatible purposes and agreed retention may be longer than purpose of collection.

11.1: The specificity of disclosure may not be useful to a regular patient. Information overload leads to individuals engaged in check box exercises and failure to focus on important elements consider streamlining disclosure with opportunity for further inquiry for those who would like to know.

15.2: While there is a role for certification requiring all entities to be certified for all services may create needless cost, burden and delay; should be as needed or appropriate.

15.4(d): The concept of reliable identification is useful, the second sentence is overly detailed and may constrain new innovation where identifier can morph over time but still link to a person. This could enhance security in case of compromise of time bound identifier. ICC recommends specifying the what, not the how.

16.5: Question as to what verification means or entails? It could be very costly and time consuming depending on interpretation.

17.1: Question whether there is any consideration of health care exchange between or with non-state actors?

17.2: Question whether patients are given access to all file elements? Dr. Notes? This may lead to files being less complete or medical notes being less forthright.

As an observer of the Council of Europe, ICC would like to thank the Council of Europe for considering these comments and remains available to work with the Council of Europe as it continues to define practical, optimally effective guidance on the protection personal data.

About The International Chamber of Commerce (ICC)

The International Chamber of Commerce (ICC) is the world's largest business organization with a network of over 6.5 million members in more than 130 countries. We work to promote international trade, responsible business conduct and a global approach to regulation through a unique mix of advocacy and standard setting activities—together with market-leading dispute resolution services. Our members include many of the world's largest companies, SMEs, business associations and local chambers of commerce.

www.iccwbo.org

@iccwbo