Strasbourg, 18 December / décembre 2017

T-PD(2017)04MosRev

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

COMITE CONSULTATIF DE LA CONVENTION POUR LA PROTECTION DES PERSONNES A L'EGARD DU TRAITEMENT AUTOMATISE DES DONNEES A CARACTERE PERSONNEL

COMPILATION OF COMMENTS ON THE DRAFT RECOMMENDATION ON THE PROTECTION OF HEALTH-RELATED DATA

COMPILATION DES COMMENTAIRES SUR LE PROJET DE RECOMMANDATION EN MATIERE DE PROTECTION DES DONNEES RELATIVES A LA SANTE

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

TABLE OF CONTENTS

GERMANY / ALLEMAGNE

Recommendation

Recommendation CM/Rec(2018)…. of the Committee of Ministers to member States on the protection of health-related data

(adopted by the Committee of Ministers … 2018, at the … meeting of the Ministers' Deputies)

Having regard to the provisions of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 (ETS No. 108, hereinafter the "Convention No. 108") and of its Additional Protocol regarding supervisory authorities and transborder data flows of 8 November 2001 (ETS No. 181), the Committee of Ministers is convinced of the desirability of facilitating the application of those principles to the processing of health-related data.

States face major challenges today, relating to the processing of health-related data, which now takes place in an environment that has changed considerably since the adoption of Recommendation (97)5 on the protection of medical data.

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

The benefits of this increasing digitisation of data can be found in numerous occasions, such as in the enhancement of public health policies, medical treatment or patients' care. The prospects of such benefits require that the advent and never-ending increase of the quantity of data, coupled to the technical analysis capacities linked to personalised health care be accompanied by legal and technical measures enabling an effective protection of every individual.

People's desire to have more control over their personal data and the decisions based on the processing of such data, the increasing involvement of patients in understanding the manner in which decisions concerning them are being taken, are additional features of this change.

Besides, geographical mobility accompanied by the development of medical devices and connected objects is also contributing 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 (97) 5 on the protection of medical data, with the more general term "health-related data" being preferred, while reaffirming the sensitivity of health-related data and the importance of regulating their use so as to guarantee due regard for the rights and fundamental freedoms of every individual, in particular the right to protection of privacy and personal data.

Health-related data are among the data belonging to a special category which, under Article 6 of Convention 108, enjoy a higher level of protection due notably to the risk of discrimination which may occur with their processing.

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

Comment [A1]: Wording! In our view: "when dealing with" would be a better formulation.

Comment [A2]: What is meant here: A person receiving care is entitled to the secrecy of professional care givers?

The processing of health-related data shall always aim serving the data subject and at enhancing the quality and efficiency of care, possibly also enhancing health systems, while respecting individuals fundamental rights.

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 (97) 5 mentioned above, are reflected in their law and practice;

- ensure, to that end, that the present Recommendation and its appendix are brought to the attention of the authorities responsible for healthcare systems, with the latter being responsible for promoting their transmission to the various actors who process health-related data, in particular healthcare professionals, data protection officers or persons having similar duties;

- 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 players who process health-related data and taken into account in the design, deployment and use of the information and communication technologies (ICTs) in that sector.

Appendix to Recommendation CM/Rec(2018)…

1.1 Chapter I. General provisions

1. Purpose

The purpose of this Recommendation is to provide member States with guidance for regulating the processing of health-related data in order to guarantee respect for the rights and fundamental freedoms of every individual, particularly the right to privacy and to protection of personal data as required by Article 8 of the European Convention on Human Rights. It also highlights to this end the importance of developing secured interoperable information systems in a manner enabling the enhancement of efficient and secured health systems.

2. Scope

This Recommendation is applicable to the processing of personal data relating to health in the public and private sectors. To this end, it also applies to the exchange and sharing of health-related data by means of digital tools. It should not be interpreted as limiting or otherwise affecting the possibility for law to grant data subjects a wider measure of protection.

The provisions of this Recommendation do not apply to health-related data processing performed by individuals in the context of purely personal or household 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 (“data subject”). An individual shall not be regarded as “identifiable” if identification requires unreasonable time, effort or resources.

- The expression “data processing” means any operation or set of operations which is performed on personal data, such as the collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure, or destruction of, or the carrying out of logical and/or arithmetical operations on such data.

- The expression “anonymisation” refers to the process applied to personal data so that the data subjects can no longer be identified either directly or indirectly.

- The expression “pseudonymisation” refers to a type of processing in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information kept separately and subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable individual. Pseudonymised data are personal data.

Comment [A3]: Wording! This sentence does not make sense like this. We again ask to make use of the well-established definitions contained in the GDPR.

- The expression “health-related data” means all personal data concerning the physical or mental

health of an individual, including the provision of healthcare services, which reveals information about this person's past, current and future health.

- The expression "genetic data" means all data relating to the genetic characteristics of an individual which have been either inherited or acquired during early prenatal development, as they result from an analysis of a biological sample from the individual concerned: chromosomal, DNA or RNA analysis or analysis of any other element enabling equivalent information to be obtained.

- The expression "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 expression "processor" means a natural or legal person, public authority, service, agency or any other body which processes data on behalf of the controller.

- The expression "reference framework" denotes a coordinated set of rules and/or processes kept constantly state-of-the-art, adapted to practice and applicable to health information systems, covering the areas of interoperability and security. Such frameworks may be given a binding nature by domestic law.

- The expression "mobile applications" denotes a set of means accessible in a mobile environment making it possible to communicate and manage health-related data remotely. It covers different forms such as connected medical objects and devices which can be used for diagnostic, treatment or wellbeing purposes among other things.

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

- The expression "data hosting" denotes the use of external data service providers irrespective of the platform used for the secure and lasting digital storage of data.

1.2 Chapter II. The legal conditions for the processing of health-related data

4. Principles concerning data processing

4.1 Anyone processing health-related data should comply with the following principles:

a. the data must be processed in a tran**sparent, lawful and fair manner**.

b. the data must be collected for explicit, specific and legitimate purposes as prescribed in principle 5 and must not be processed in a manner which is incompatible with these purposes. Further processing for archiving purposes in the public interest, for scientific or historical research purposes or statistical purposes is not regarded as incompatible with the initial purposes, where appropriate guarantees enable rights and fundamental freedoms to be respected.

c. The processing of data should be proportionate in relation to the legitimate purpose pursued and shall be carried out only on the basis of consent of the data subject as laid down in principle 5.2 or on other legitimate basis as laid down in other paragraphs of principle 5.

d. Personal data should, in principle and as far as possible, be collected from the data subject. Where the data subject is not in a capacity to provide the data and such data are necessary for the purposes of the processing, they can be collected from other sources in accordance with the principles of this ~~recommendation~~Recommendation.

e. The data must be adequate, relevant and not excessive in relation to the purposes for which they are processed; they must be accurate and, if necessary, kept up to date.

f. Appropriate security measures, taking into consideration the latest technological developments, the sensitive nature of health-related data and the assessment of potential risks, should be established to prevent risks such as accidental or unauthorised access to, destruction, loss, use,

Comment [A4]: This definition is not correct yet. A "doctor" is certainly a "health professional". But he does not co-ordinate the treatment necessarily, but often treats the patient/individual directly. Therefore, the word co-ordination is misleading as many health professionals are not directly involved in the co-ordination of care (nurses, pharmacists, physiotherapists etc.)

Comment [A5]: This term does not appear again in the document. Is there a need for this definition?

unavailability, inaccessibility, modification or disclosure of personal data.

g. The rights of the person whose data are processed must be respected, particularly the rights of access to the data, information, rectification, objection, deletion and portability as prescribed in principle 12 of the present recommendation.

4.2 Personal data protection principles must be taken into account by default and incorporated right from the design of information systems which process health-related data. Compliance with these principles should be regularly reviewed throughout the life cycle of the processing (privacy by design). The controller should carry out, before commencing the processing and at regular intervals, an assessment of the potential impact of the processing of data foreseen in terms of data protection and respect for privacy.

4.3 Data controllers and the processors acting under their responsibility should take all appropriate measures to fulfil their obligations with regard to data protection and should be able to demonstrate in particular to the competent supervisory authority that the processing is in line with those obligations.

4.4 Data controllers and their processors who are not health professionals should only process health-related data in accordance with rules of confidentiality and security measures that ensure a level of protection equivalent to the one imposed to health professionals.

5. Legitimate basis of health-related data processing

5.1 Health-related data may only be processed where appropriate safeguards are enshrined in law and the processing is necessary for:

a. preventive medical purposes and purposes of medical diagnosis, administration of care or treatment, or management of health services by health professionals and those of the social and medico-social sector, subject to the conditions defined by law;

b. reasons of public health, such as for example protection against health hazards, humanitarian action or in order to ensure a high standard of quality and safety for medical treatment, health products and medical devices, subject to the conditions defined by law;

c. the purpose of safeguarding the vital interests of the data subject or of another person where consent cannot be collected;

d. reasons of public interest in the field of managing claims for social welfare and health insurance benefits and services, subject to the conditions defined by law;

e. processing for archiving purposes in the public interest, for scientific or historical research purposes or statistical purposes subject to the conditions defined by law ~~(such as for instance the obligation of prior information of the data subject to enable the exercise of the right to refuse participation in a scientific research)~~ in order to guarantee protection of the data subject's fundamental rights and legitimate interests;

f. 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 law or any collective agreement complying with the said law;

g. reasons essential to the recognition, exercise or defence of a legal claim~~.~~;

~~g.~~h. reasons of substantial public interest if the law is proportionate to the aim pursued, respects the essence of the right to data protection and provides for suitable und specific measures to safeguard the fundamental rights and the interests of the data subject.

Comment [A6]: The controller's obligation to inform the data subject is dealt with in principle 11, not in principle 12.

Comment [A7]: If the addition "of the present recommendation" is used, is should be done everywhere in the document. However, the document often only speaks of the „recommendation" or „this recommendation". The same wording should be used or is something else meant?

Comment [A8]: The GDPR differs between the obligation of the controller to respect privacy by default and privacy by design. The producer, however, is only encouraged to respect privacy by default and by design. This Recommendation should not be stricter than the GDPR which contains these new principles of privacy law.

Comment [A9]: The sentence before the brackets does not describe privacy by design.

Comment [A10]: This example should be deleted here. The rather complicated questions (obligation to inform and "right to say no") should be dealt with in Chapter 5. Although there is - in general - the obligation to inform the data subject before processing, there are exceptions of this obligation if certain conditions are fulfilled. In addition to that, although the data subject has - in general - the "right to say no" to processing for scientific purposes, this right is not granted without exceptions.

Comment [A11]: In line with Article 9 § 2 letter g of the GDPR.

5.2 Health-related data may also be processed if the data subject has given her or his consent, except in cases where domestic law provides that a ban on health-related data processing cannot be lifted solely by the data subject's consent. Where consent of the data subject to the processing of health-related data is required, in accordance with domestic law, it should be free, specific, informed and explicit. Consent can be expressed by electronic means.

5.3 Health-related data may also be processed where the processing is necessary for the execution of a contract entered into by the data subject or on his or her behalf with a health professional subject to conditions defined by law, including the obligation of secrecy.

5.4 In all cases, appropriate safeguards should be established in order to guarantee, in particular, the security of the 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 unborn children

Health-related data concerning unborn children, inter alia such as data resulting from a prenatal diagnosis or from the identification of the genetic characteristics of such children should enjoy an appropriate protection.

7. Genetic data

7.1 Genetic data should only be collected subject to appropriate safeguards and where it is either prescribed by domestic law or on the basis of the consent expressed by the data subject, except where consent is excluded by domestic law as legal basis for the processing of genetic data..

7.2 Genetic data processed with a preventive aim, for diagnosis or for treatment of the data subject or a member of her or his biological family or for scientific research should be used only for these purposes or to enable the persons concerned by the results of such tests to take an informed decision on these matters.

7.3 Processing of genetic data for the purpose of a judicial procedure or investigation should be used only when there are no alternative or less intrusive means to establish whether there is a genetic link in the context of the production of evidence, to prevent a real and immediate danger or to for the prosecution of a specific criminal offence. Such data should not be used to determine other characteristics which may be linked genetically, except where domestic law provides for it with appropriate safeguards.

7.4 Any processing of genetic data prescribed by law other than in the cases provided for in paragraphs 7.2 and 7.3 should only be carried out to avoid any serious prejudice to the health of the data subject or of a member of her or his biological family or for reasons in relation with humanitarian action.

7.5 Existing predictive data resulting from genetic tests should not be processed for insurance purposes, except where this is specifically provided for by domestic law. In that case, their processing should only be authorised in full respect of the applicable criteria defined by law, in light of the type of test used and the particular risk concerned. The provisions of Recommendation (2016)8 on the processing of personal health-related data for insurance purposes, including data resulting from genetic tests are also to be taken into consideration in that regard.

7.6 The data subject is entitled to know any information collected about her or his health. However, the wish of the person whose genetic data are analysed not to know should be taken into consideration, and that person should be informed, prior to such analysis, of the possibility of not being informed of the results, including of unexpected findings. Her or his wish not to know may, in her or his interests or in the interests of a member of her or his biological family, have to be restricted as foreseen by law, notably in light of the doctors' duty to provide care.

8. Sharing of health-related data for purposes of providing and administering health care

8.1 Where health-related data are shared by different professionals for purposes of providing and

Comment [A12]: It should be stated at the beginning of this paragraph that there always needs to be a legal basis for "sharing" health-related data because this is a form of processing.

administering health care of an individual, the data subject shall be informed beforehand, except where this proves to be impossible due to an emergency, of the nature of the health-related data processed and of the health professionals participating in the provision of care. The data subject must be able, in accordance with safeguards prescribed by law, to withdraw consent, where such consent is required by law, or object at any time to the exchange and sharing of her or his health-related data.

8.2 Professionals operating on a particular individual case in the health and medico-social sector and sharing data in the interests of greater co-ordination should be subject to professional confidentiality incumbent upon a health-care professional, or to equal rules of confidentiality.

8.3 The exchange and sharing of data between health professionals should be limited to the information strictly necessary for the co-ordination or continuity of care, prevention or medico-social and social follow-up of the individual, with the respective actors only able in this case to share or receive data lying strictly within the scope of their tasks and depending on their authorisations. Appropriate measures should be taken to ensure the security of the data.

8.4 The use of an electronic medical file and of an electronic mailbox allowing for the sharing and exchange of health-related data should respect those principles.

9. Communication of health-related data

9.1 Health-related data may be communicated to recipients where the latter are authorised by law to have access to the data.

9.2 Insurance companies and employers cannot, in principle, be regarded as recipients authorised to have access to the health-related data of patients unless domestic law makes provision for this with appropriate safeguards and if the data subject has validly consented to it.

9.3 Health-related data will, unless other appropriate safeguards are provided for by law, only be communicated to an authorised recipient who is subject to the rules of confidentiality incumbent upon a health-care professional, or to equal rules of confidentiality.

10. Storage of health-related data

The data should not be stored in a form which permits identification of the data subjects for longer than is necessary for the purposes for which they are processed unless they are used for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes and where appropriate measures enable to safeguard the rights and fundamental freedoms of the data subject. In this case, data should in principle be anonymised as soon as the research, the archiving activity or the statistical study enables it.

1.3 Chapter III. The rights of the data subject

11. Transparency of processing

11.1 The data subject must be informed by the controller of the processing of their health-related data.

The information must include:

- 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,
- the length of preservation of the data,
- the recipients or categories of recipients of the data, and planned data transfers to a third country, or an international organisation,
- the possibility, if applicable, of objecting to the processing of their data, in the conditions prescribed in paragraph 12.2,

- the conditions and the means made available to them for exercising via the controller their rights of access, the right of rectification and the right to erasure of their health-related data.

The information must where necessary, with a view to ensuring a fair and transparent processing, also include:

- that their data may subsequently be processed for a compatible purpose, in accordance with appropriate safeguards provided for by domestic law and in the conditions prescribed in paragraph 4.1.b,
- the specific techniques used to process their health-related data,
- the possibility of lodging a complaint with a supervisory authority,
- the existence of automated decisions, including profiling which is only permissible where prescribed by law and subject to appropriate safeguards.

11.2 This information should be provided prior to data collection or at the first communication, unless it proves impossible or requires disproportionate efforts from the controller, in particular for processing for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes.

11.3 The information must be intelligible and easily accessible, in a clear and plain language and suited to the circumstances to allow a full understanding of the processing by the data subject. In particular, where the data subject is physically or legally incapable of receiving the information, it may be given to the person legally representing her or him. If a legally incapacitated person is capable of understanding, he or she should be informed before the data are processed.

11.4 Only urgency or the impossibility for the data subject to be informed can give rise to an exemption from the obligation of informing. In such a case, information should be provided as soon as possible.

11.5 A person's wish to be kept in ignorance of a diagnosis or prognosis should be complied with, except where this constitutes a serious risk for the health of third parties.

11.6 Domestic law should provide for appropriate safeguards ensuring respect for these rights.

12. The rights of access, objection, rectification, erasure and data portability

Comment [A13]: The Convention 108 (and the current version of the Amending Protocol as well) do not contain a right to data portability.

12.1 The data subject has the right to know whether personal data which concern her or him are being processed, and, if so, to obtain - without excessive delay or expense and in an intelligible form - communication of her or his data and to have access in the same conditions to at least the following information:

- the purpose or purposes of the processing,
- the categories of personal data concerned,
- the recipients or categories of the recipients of the data and the envisaged data transfers to a third country, or an international organisation,
- the preservation period,
- the knowledge of the reasoning underlying data processing where the results of such processing are applied to her or him, notably in the case of profiling.

12.2 The data subject has the right to erasure of data processed ~~against~~ in violation of the principles of this Recommendation. The data subject is entitled to obtain rectification of data concerning her or him. The data subject furthermore has the right to object on grounds relating to her or his personal situation to the processing of her or his health-related data, unless it is anonymised or the controller demonstrates an overriding and legitimate reason for pursuing the data processing.

12.3 If the request to rectify or erase the data is refused or if the data subject's objection is rejected, he or she should be able to have a remedy.

12.4 The right to data portability requires, subject to conditions prescribed by law, from the controller, where the processing is performed by automatic means, the transmission - in a structured, interoperable and machine-readable format - of her or his personal data with a view to transmitting

them to another controller. The data subject can also require from the controller that he or she transmits directly the data to another controller.

12.5 The rights of data subjects should be easy to exercise. ~~and all States should ensure that every person is given the necessary and adequate,means to exercise their rights.~~

12.6 Health professionals have to put in place all necessary measures in order to ensure respect for the effective exercise of such rights as an element of their professional deontology, as recognised by domestic law.

12.7 The rights of data subjects can be subject to restrictions provided for by law, where such restrictions are necessary and proportionate measures in a democratic society for the reasons specified in Article 9 of Convention 108, notably objectives of general public interest of the State relating to public health.

1.4 Chapter IV. Security and interoperability

13. Security

13.1 The processing of health-related data is to be made secure and security measures adapted to the risks for fundamental rights and freedoms must in that regard be defined to ensure that all players observe high standards guaranteeing the lawfulness of the processing and security and confidentiality of such data.

13.2 These security rules, defined by domestic law and possibly contained in reference frameworks, constantly kept state-of-the-art and regularly reviewed, should result in the adoption of technical and organisational measures as to protect personal health-related data from any illegal or accidental destruction, any loss or any impairment, and to guard against any unauthorised access or unavailability or inaccessibility. In particular, the law should make provision for organising and regulating procedures concerning the collection, storage and restitution of health-related data.

13.3 System availability – i.e. the proper functioning of the system – 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.

13.4 Guaranteeing integrity requires verification of every action carried out on the data, any changes made to or deletion of data, including the communication of data. It also requires the establishment of measures to monitor access to the data base and the data themselves, ensuring that only authorised persons are able to access the data.

13.5 Auditability should lead to a system making it possible to trace any access to the information system and modifications made and for any action carried out, to be able to identify its author.

13.6 Activity entailing hosting health-related data and making them available for users should comply with the security reference framework and principles of personal data protection.

13.7 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-related data. They must have full regard for professional secrecy and comply with appropriate measures laid down in law to guarantee the confidentiality and security of the data.

14. Interoperability

14.1 Interoperability of systems enables to contribute to data portability and should for this reason be encouraged. Reference frameworks, offering a technical frame, facilitating interoperability based on international norms should ensure that a high level of security is guaranteed while providing for such interoperability. The monitoring of the implementation of reference frameworks can be done through certification schemes.

Comment [A14]: There is no right to data portability under the Convention 108.

Comment [A15]: What does that mean concretely?

Comment [A16]: What is the scope of this chapter?
Security of processing and Interoperability of data or interoperability of technical and organisational measures to ensure secure processing?

Comment [A17]: The responsible party for implementation of security measures should be stated here, e.g.: "The data controller and the processor should implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk."

Comment [A18]: The reference is not clear: What are "these security rules"? Principles relating to the processing of health data set out by law, technical guidelines for choosing adequate security measures, codes of conduct or the specific technical and organisational security measures to be implemented by the controller and/or the processor?

Comment [A19]: What does this mean? Should specific technical measures be prescribed by law? Or may "domestic law" give existing reference frameworks a "binding nature"?

Comment [A20]: What does that word is supposed to mean here?

Comment [A21]: What does this mean? They must be subject to a duty of professional secrecy?

Comment [A22]: What does this mean?

14.2 Reference frameworks should be taken into consideration at the design stage of information systems.

1.5 Chapter V. Scientific research

15. Scientific research

15.1 The processing of health-related data for the purposes of scientific research should be subject to appropriate safeguards, complementing the other provisions of the present recommendation, and be carried out with a legitimate aim ~~for~~ and in compliance with the rights and fundamental freedoms of the data subject.

15.2 The need to process health-related data for the purposes of scientific research should be evaluated in the light of the aim pursued and the risks to the data subject and, in relation to genetic data to her or his biological family.

15.3 The data subject should, in addition to what is foreseen in Chapter III be provided with prior, transparent and comprehensible information that is as precise as possible with regard to:

- the nature of the envisaged scientific research, the possible choices that he or she could exercise as well as any relevant conditions governing the use of the data, including re-contact and feedback;
- the conditions applicable to the storage of the data, including access and possible communication policies; and
- the rights and safeguards provided for by law, and specifically of her or his right to refuse to participate in the research and withdraw at any time.

Restrictions may be applied in the event of a medical emergency provided that appropriate safeguards are ensured.

15.4 As it is not always possible to determine beforehand the purposes of different research projects at the time of the collection of data, data subjects should be able to ~~exercise a choice~~express consent ~~solely~~ for certain areas of research or certain parts of research projects, to the extent allowed by the intended purpose, with due regard for recognised ethical standards.

15.5 Health-related data should only be used in a research project if the data subject, after having received prior information according to the provisions of paragraph 15.3, has consented to it or, if permitted by law providing appropriate safeguards, has not objected to it. If the proposed use of the data in a research project is not explained prior to collection of the data, reasonable efforts should be made to contact the data subject. The wish of the data subject not to be contacted should be observed. Where the attempt to contact the data subject proves unsuccessful, the health-related data should only be used in the research project subject to an independent evaluation of the fulfillment of the following conditions:

a. evidence is provided that reasonable efforts have been made to contact the person concerned;

b. the research addresses an overriding scientific interest and the processing is proportionate to the objective pursued ;

c. the aims of the research could not reasonably be achieved without using the data for which consent cannot be obtained; and

d. there is no evidence that the person concerned has expressly opposed such research use.

15.6 The conditions in which health-related data are processed for scientific research must be assessed, where necessary, by the body or bodies designated by law.

Comment [A23]: It needs to be clarified that it does not need to be a legitimate aim for the rights or freedoms of the data subject, but that the aim must not compromise these rights and freedoms.

Comment [A24]: Please give examples! It is not understandable that research by processing of health-related data needs to be done in the case of a medical emergency.

Comment [A25]: More precise.

Comment [A26]: This word needs to be deleted because data subjects are, of course, not prevented from expressing consent for specific research purposes.

Comment [A27]: Germany cannot accept 15.5 the way it is formulated at the moment. The text is - for a large part - a copy-paste of the Recommendation (2016)6 on research on biological materials of human origins. This Recommendation, however, only deals with health-related data.

Moreover, the current text of 15.5 mixes different questions leading to misunderstandings and imprecisions:

1. Legal basis for processing (consent; law):

2. Possibilities to stop or to prevent the processing (withdrawal of consent; objection in case processing is based on law);

3. The obligation to inform the data subject.

It is highly recommended to deal with these different issues in separate numbers.

In addition to that, the current text is imprecise in several ways:

1. According to EU law there are - under certain conditions - exceptions possible in domestic law from the right to object in cases where the processing for scientific research purposes is based on law (see Article 89 § 2 of the GDPR which allows for restrictions of the right to object contained in Article 21 of the GDPR).

2 The right to be informed is not granted without exceptions in the area of research, e.g. if the data are not collected from the data subject and a number of safeguards are in place (see in detail Article 14 § 5 letter b of the GDPR).

3. It is not understandable why there should be an independent evaluation in the cases mentioned in the text. This requirement does not exist in EU law. We do not see a need to come up with this requirement here.

...

15.7 Healthcare professionals who are entitled to carry out their own medical research and scientists in other disciplines should be able to use the health-related data which they hold as long as the data subject has been informed of this possibility beforehand in compliance with paragraph 15.3 and subject to complementary safeguards determined by law such as requiring explicit consent or the assessment of the competent body designated by law.

15.8 Where the scientific research purposes allow~~possible~~, data should be anonymised and where research purposes do not allow~~it is not possible~~, pseudonymisation of the data, with intervention of a trusted third-party at the separation stage of the identification, is among the measures that should be implemented to safeguard the rights and fundamental freedoms of the data subject. This must be done where the purposes of the scientific research can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects.

Comment [A28]: Necessary clarification. The question is not the mere (e.g. technical) possibility of anonymisation or pseudonymisation, but whether the achievement of research purposes might be impaired.

15.9 Where a data subject withdraws from a scientific research, her or his health-related data processed in the context of that research should be destroyed or anonymised in a manner not to compromise the scientific validity of the research and the data subject should be informed accordingly.

15.10 Personal data used for scientific research should not be published in a form which enables the data subjects to be identified, except where he or she has consented to it ~~and~~ or domestic law allows it.

Comment [A29]: Not in line with GDPR and the new German Data Protection Law (Section 27 § 4 Bundesdatenschutzgesetz 2018).
The possibility to publish without consent is necessary
if doing so is indispensable for the presentation of research findings on contemporary events.

1.6 Chapter VI – Mobile applications

16. Mobile applications

16.1 Where the data collected by these applications, whether implanted on the person or not, may reveal information on the physical or mental state of a person in connexion with her or his health or concern any information regarding health care and medico-social provision, they constitute health-related data. In this connection they enjoy the same legal protection and confidentiality applicable to other health-related data processing as defined by the present Recommendation and, where applicable, supplemented by the domestic law.

16.2 Persons using such mobile applications, as soon as they involve the processing of their personal data, must enjoy the same rights as those provided for in Chapter III of the present Recommendation. They must notably have obtained beforehand all necessary information on the nature and functioning of the system in order to be able to control its use. To this effect clear and transparent information on the intended processing should be drafted by the controller with the participation of the software designer and the software distributor whose respective roles have to be determined in advance.

16.3 Any use of mobile applications must be accompanied by specific, tailored and state-of-the-art security measures which notably provide for the authentication of the person concerned and the encryption of the transmission of data.

16.4 The hosting, by a third party of health-related data produced by mobile applications must obey security rules providing for the confidentiality, integrity and restitution of the data upon request of the data subject.

ITALY / ITALIE

Recommendation

Recommendation CM/Rec(2018)…. of the Committee of Ministers to member States on the protection of health-related data

(adopted by the Committee of Ministers … 2018, at the … meeting of the Ministers' Deputies)

Having regard to the provisions of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 (ETS No. 108, hereinafter the "Convention No. 108") and of its Additional Protocol regarding supervisory authorities and transborder data flows of 8 November 2001 (ETS No. 181), the Committee of Ministers is convinced of the desirability of facilitating the application of those principles to the processing of health-related data.

States face major challenges today, relating to the processing of health-related data, which now takes place in an environment that has changed considerably since the adoption of Recommendation (97)5 on the protection of medical data.

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

The benefits of this increasing digitisation of data can be found in numerous occasions, such as in the enhancement of public health policies, medical treatment or patients' care. The prospects of such benefits require that the advent and never-ending increase of the quantity of data, coupled to the technical analysis capacities linked to personalised health care be accompanied by legal and technical measures enabling an effective protection of every individual.

People's desire to have more control over their personal data and the decisions based on the processing of such data, the increasing involvement of patients in understanding the manner in which decisions concerning them are being taken, are additional features of this change.

Besides, geographical mobility accompanied by the development of medical devices and connected objects is also contributing 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 (97) 5 on the protection of medical data, with the more general term "health-related data" being preferred, while reaffirming the sensitivity of health-related data and the importance of regulating their use so as to guarantee due regard for the rights and fundamental freedoms of every individual, in particular the right to protection of privacy and personal data.

Health-related data are among the data belonging to a special category which, under Article 6 of Convention 108, enjoy a higher level of protection due notably to the risk of discrimination which may occur with their processing.

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

The processing of health-related data shall always aim at serving the data subject and ~~at~~ enhancing the quality and efficiency of care, possibly also enhancing health systems, while respecting individuals' fundamental rights.

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 (97) 5 mentioned above, are reflected in their law and practice;
- ensure, to that end, that the present Recommendation and its appendix are brought to the attention of the authorities responsible for healthcare systems, with the latter being responsible for promoting their transmission to the various actors who process health-related data, in particular healthcare professionals, data protection officers or persons having similar duties;

- 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 players who process health-related data and taken into account in the design, deployment and use of the information and communication technologies (ICTs) in that sector.

Appendix to Recommendation CM/Rec(2018)…

1.7 Chapter I. General provisions

1. Purpose

The purpose of this Recommendation is to provide member States with guidance for regulating the processing of health-related data in order to guarantee respect for the rights and fundamental freedoms of every individual, particularly the right to privacy and to protection of personal data as required by Article 8 of the European Convention on Human Rights~~. It also highlights to this end the importance of developing secured interoperable information systems in a manner enabling the enhancement of efficient and secured health systems~~.

Comment [A30]: Especially now that the section on interoperability has been reduced, this sentence may not be necessary as interoperability is one of the (many) elements of this Recommendation

2. Scope

This Recommendation is applicable to the processing of personal data relating to health in the public and private sectors. To this end, it also applies to the exchange and sharing of health-related data by means of digital tools. It should not be interpreted as limiting or otherwise affecting the possibility for ~~domestic~~ law to grant data subjects a wider [~~measure of~~] protection.

Comment [A31]: Does it work in English?

~~To this end, it also applies to the exchange and sharing of health-related data by means of digital tools. Such tools should be designed to ensure respect for the rights and fundamental freedoms of individuals.~~

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

Comment [A32]: EM should give further explanations in line with the EM of the modernised Convention

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 (“data subject”). An individual shall not be regarded as “identifiable” if identification requires unreasonable time, effort or resources.

- The expression “data processing” means any operation or set of operations which is performed on personal data, such as the collection, ~~-~~storage, preservation, alteration, retrieval, disclosure, making available, erasure, or destruction of, or the carrying out of logical and/or arithmetical operations on such data.

- The expression “anonymisation” refers to the process applied to personal data so that the data subjects can no longer be identified either directly or indirectly.

- The expression “pseudonymisation” refers to a type of processing ~~which makes it possible to process~~ in such a manner that the personal data can no longer be attributed to a specific data subject

without the use of additional information kept separately and subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable individual. Pseudonymised data are personal data.

- The expression “health-related data” means all personal data concerning the physical or mental health of an individual, including the provision of healthcare services, which reveals information about this person’s past, current and future health.

- The expression “genetic data” means all data relating to the genetic characteristics of an individual which have been either inherited or acquired during early prenatal development, as they result from an analysis of a biological sample from the individual concerned: chromosomal, DNA or RNA analysis or analysis of any other element enabling equivalent information to be obtained.

~~- The expression “data processing” means any operation or set of operations which is performed on personal data, such as the collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure, or destruction of, or the carrying out of logical and/or arithmetical operations on such data.~~

- The expression “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 expression “processor” means a natural or legal person, public authority, service, agency or any other body which processes data on behalf of the controller.

- The expression "reference framework" denotes a coordinated set of rules and/or processes kept constantly state-of-the-art, adapted to practice and applicable to health information systems, covering the areas of interoperability and security. Such frameworks may be given a binding nature by domestic law.

- The expression "mobile applications" denotes a set of means accessible in a mobile environment making it possible to communicate and manage health-related data remotely. It covers different forms such as connected medical objects and devices which can be used for diagnostic, treatment or wellbeing purposes among other things.

- The expression “health professionals” covers all professionals recognised as such by domestic law practising in the health, medical welfare or social welfare sector, bound by a confidentiality obligation and involved in ~~co-ordinating~~ treatment for an individual to whom they provide health care.

Comment [A33]: Health professionals can either be or not involved in a co-ordinated treatment

- The expression "data hosting" denotes the use of external data service providers irrespective of the platform used for the secure and lasting digital storage of data.

1.8 Chapter II. The legal conditions for the processing of health-related data

4. Principles concerning data processing

4.1 Anyone processing health-related data should comply with the following principles:

a. the data must be processed in a tran**sparent, lawful and fair manner**.

b. the data must be collected for explicit, specific and legitimate purposes as prescribed in principle 5 and must not be processed in a manner which is incompatible with these purposes. Further processing for archiving purposes in the public interest, for scientific or historical research purposes or statistical purposes is not regarded as incompatible with the initial purposes, where appropriate guarantees enable rights and fundamental freedoms to be respected.

c. The processing of data should be proportionate in relation to the legitimate purpose pursued and shall be carried out only on the basis of consent of the data subject as laid down in principle 5.2 or on other legitimate basis as laid down in other paragraphs of principle 5.

d. Personal data should, in principle and as far as possible, be collected from the data subject. Where the data subject is not in a capacity to provide the data and such data are necessary for the

purposes of the processing, they can be collected from other sources in accordance with the principles of this recommendation.

e. The data must be adequate, relevant and not excessive in relation to the purposes for which they are processed; they must be accurate and, if necessary, kept up to date.

f. Appropriate security measures, taking into consideration the latest technological developments, the sensitive nature of health-related data and the assessment of potential risks, should be established to prevent risks such as accidental or unauthorised access to, destruction, loss, use, unavailability, inaccessibility, modification or disclosure of personal data.

g. The rights of the person whose data are processed must be respected, particularly the rights of access to the data, information, rectification, objection, deletion and portability as prescribed in principle 12 of the present recommendation.

4.2 Personal data protection principles must be taken into account by default and incorporated right from the design of information systems which process health-related data. Compliance with these principles should be regularly reviewed throughout the life cycle of the processing (privacy by design). The controller should carry out, before commencing the processing and at regular intervals, an assessment of the potential impact of the processing of data foreseen in terms of data protection and respect for privacy.

4.3 Data controllers and the processors acting under their responsibility should take all appropriate measures to fulfil their obligations with regard to data protection and should be able to demonstrate in particular to the competent supervisory authority that the processing is in line with those obligations.

4.4 Data controllers and their processors who are not health professionals should only process health-related data in accordance with rules of confidentiality and security measures that ensure a level of protection equivalent to the one imposed to health professionals.

5. ~~Purposes and l~~Legitimate basis of health-related data processing

5.1 Health-related data may only be processed where appropriate safeguards are enshrined in law and ~~provided and~~ the processing is necessary ~~for one of the following purposes~~for:

~~h.~~i. ~~for~~ preventive medical purposes and ~~for~~ purposes of medical diagnosis, administration of care or treatment, or management of health services by health professionals and those of the social and medico-social sector, subject to the conditions defined by ~~domestic~~ law;

~~i.~~j. ~~for~~ reasons of public health, such as for example protection against health hazards, humanitarian action or in order to ensure a high standard of quality and safety for medical treatment, health products and medical devices, subject to the conditions defined by ~~domestic~~ law;

~~j.~~k. ~~for~~ the purpose of safeguarding the vital interests of the data subject or of another person where consent cannot be collected;

~~k.~~l. ~~for~~ reasons of public interest in the field of managing claims for social welfare and health insurance benefits and services, subject to the conditions defined by ~~domestic~~ law;

~~l. [for reasons of public health compatible with the initial purpose of the collection of data, provided that they are lawful and legitimate, subject to the conditions defined by domestic law;]~~

m. ~~for~~ processing for archiving purposes in the public interest, for scientific or historical research purposes or statistical purposes subject to the conditions defined by ~~domestic~~ law (such as for instance the obligation of prior information of the data subject to enable the exercise of the right to refuse participation in a scientific

research) in order to guarantee protection of the data subject's fundamental rights and legitimate interests;

n. ~~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~~ law or any collective agreement complying with the said law;

o. ~~for~~ reasons essential to the recognition, exercise or defence of a legal claim.

5.2 Health-related data may also be processed if the data subject has given her or his consent, except in cases where domestic law provides that a ban on health-related data processing cannot be lifted solely by the data subject's consent. Where consent of the data subject to the processing of health-related data is required, in accordance with domestic law, it should be free, specific, informed and explicit. Consent can be expressed by electronic means.

Comment [A34]: Do we need this?

5.3 Health-related data may also be processed where the processing is necessary for the execution~~based on~~ of a contract entered into by the data subject or on his or her behalf with a health professional subject to conditions defined by law, including the obligation of secrecy.

5.4 In all cases, appropriate safeguards should be established in order to guarantee, in particular, the security of the 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 unborn children

Health-related data concerning unborn children, inter alia such as data resulting from a prenatal diagnosis or from the identification of the genetic characteristics of such children should enjoy an appropriate protection.

7. Genetic data

7.1 Genetic data should only be collected subject to appropriate safeguards and where it is either prescribed by law~~,~~ or on the basis of the consent expressed by the data subject, except where consent is excluded by law as legal basis for the processing of genetic data. ~~where this is required by law, and subject to appropriate safeguards.~~

7.2 Genetic data processed with a preventive aim, for diagnosis or for treatment of the data subject or a member of her or his biological family or for scientific research should be used only for these purposes or to enable the persons concerned by the results of such tests to take an informed decision on these matters.

7.3 Processing of genetic data for the purpose of a judicial procedure or investigation should be used only when there are no alternative or less intrusive means to establish whether there is a genetic link in the context of the production of evidence, to prevent a real and immediate danger or ~~to~~ for the prosecution of a specific criminal offence. Such data should not be used to determine other characteristics which may be linked genetically, except where domestic law provides for it with appropriate safeguards.

7.4 Any processing of genetic data prescribed by law other than in the cases provided for in paragraphs 7.2 and 7.3 should only be carried out to avoid any serious prejudice to the health of the data subject or of a member of her or his biological family or for reasons in relation with humanitarian action.

7.5 Existing predictive data resulting from genetic tests should not be processed for insurance purposes, except where this is specifically provided for by law. In that case, their processing should only be authorised in full respect of the applicable criteria defined by law, in light of the type of test used and the particular risk concerned. The provisions of Recommendation (2016)8 on the processing of personal health-related data for insurance purposes, including data resulting from genetic tests are also to be taken into consideration in that regard.

7.6 The data subject is entitled to know any information collected about her or his health. However, the wish of the person whose genetic data are analysed not to know should be taken into consideration, and that person should be informed, prior to such analysis, of the possibility of not being informed of the results, including of unexpected findings. Her or his wish not to know may, in her or his interests or in the interests of a member of her or his biologic family, have to be restricted as foreseen by law, notably in light of the doctors' duty to provide care.

~~7.7 The publication of genetic data which would identify the data subject or a person who has a direct link with her or his genetic line, should be prohibited, except where the data subject has expressly consented beforehand to it and it is prescribed by law, for specific purposes and with the appropriate safeguards.~~

8. Shar~~ed professional secrecy~~ing of health-related data for purposes of providing and administering health care

8.1 Where health-related data are shared by different professionals for purposes of providing and administering health care of an individual, the data subject ~~should~~ shall be informed beforehand, except where this proves to be impossible due to an emergency, of the nature of the health-related data processed and of the health professionals participating in the provision of care. The data subject must be able, in accordance with safeguards prescribed by law, to withdraw consent, where such consent is required by law, or object at any time to the exchange and sharing of her or his health-related data.

8.2 ~~In the interests of greater co-ordination between p~~Professionals operating on a particular individual case in the health and medico-social sector and sharing data in the interests of greater co-ordination should be subject to professional confidentiality incumbent upon a health-care professional, or to equal rules of confidentiality~~, the domestic law should recognise a shared professional secrecy, between professionals who are themselves legally bound by such secrecy~~.

Comment [A35]: At least in the EM we should underline that the coordination should aim at enhancing the health care of the individual

8.3 The exchange and sharing of data between health professionals should be limited to the information strictly necessary for the co-ordination or continuity of care, prevention or medico-social and social follow-up of the individual, with the respective actors only able in this case to share or receive data lying strictly within the scope of their tasks and depending on their authorisations. Appropriate measures should be taken to ensure the security of the data.

8.4 The use of an electronic medical file and of an electronic mailbox allowing for the sharing and exchange of health-related data should respect those principles.

9. Communication ~~to 'authorised recipients'~~ of health-related data

9.1 Health-related data may be communicated to recipients where the latter are authorised by ~~domestic~~ law to have access to the data. ~~Such authorised recipients may be judicial authorities, experts appointed by a court authority, members of staff of an administrative authority designated by a legal formal act or humanitarian organisations, among other people.~~

9.2 ~~Medical officers of i~~Insurance companies and employers cannot, in principle, be regarded as recipients authorised to have access to the health-related data of patients unless domestic law makes provision for this with appropriate safeguards and if the data subject has validly consented to it.

Comment [A36]: Is it the correct wording?

9.3 Health-related data will, unless other appropriate safeguards are provided for by ~~domestic~~ law, only be communicated to an authorised recipient who is subject to the rules of confidentiality incumbent upon a health-care professional, or to equal rules of confidentiality.

10. Storage of health-related data

The data should not be stored in a form which permits identification of the data subjects for longer than is necessary for the purposes for which they are processed unless they are used for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes and where appropriate measures enable to safeguard the rights and fundamental freedoms of the data subject. In this case, data should in principle be

anonymised as soon as the research, the archiving activity or the statistical study enables it.

1.9 Chapter III. The rights of the data subject

11. Transparency of processing

11.1 The data subject must be informed by the controller of the processing of their health-related data.

The information must include:

- 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,
- the length of ~~conservation~~ preservation of the data,
- the recipients or categories of recipients of the data, and planned data transfers to a third country, or an international organisation,
- the possibility, if applicable, of objecting to the processing of their data, in the conditions prescribed in paragraph 12.2,
- the conditions and the means made available to them for exercising via the controller their rights of access, the right of rectification and the right to erasure of their health-related data.

The information must where necessary, with a view to ensuring a fair and transparent processing, also include:

- that their data may subsequently be processed for a compatible purpose, in accordance with appropriate safeguards provided for by domestic law and in the conditions prescribed in paragraph 4.1.b,
- the specific techniques used to process their health-related data,
- the possibility of lodging a complaint with a supervisory authority,
- the existence of automated decisions, including profiling ~~where~~ which is only permissible where prescribed by~~domestic~~ law ~~allows~~ and~~it~~ subject to appropriate safeguards.

11.2 This information should be provided prior to data collection or at the first communication, unless it proves impossible or requires disproportionate efforts from the controller, in particular for processing for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes.

11.3 The information must be intelligible and easily accessible, in a clear and plain language and suited to the circumstances to allow a full understanding of the processing by the data subject. In particular, where the data subject is physically or legally incapable of receiving the information, it may be given to the person legally representing her or him. If a legally incapacitated person is capable of understanding, he or she should be informed before the data are processed.

11.4 Only urgency or the impossibility for the data subject to be informed can give rise to an exemption from the obligation of informing. In such a case, information should be provided as soon as possible.

11.5 A person's wish to be kept in ignorance of a diagnosis or prognosis should be complied with, except where this constitutes a serious risk for the health of third parties.

11.6 Domestic law should provide for appropriate safeguards ensuring respect for these rights.

12. The rights of access, objection, rectification, erasure and data portability

12.1 The data subject has the right to know whether personal data which concern her or him are being processed, and, if so, to obtain - without excessive delay or expense and in an intelligible form - communication of her or his data and to have access~~, without excessive delay or expense and in an intelligible form,~~ in the same conditions to at least the following information:

- the purpose or purposes of the processing,
- the categories of personal data concerned,
- the recipients or categories of the recipients of the data and the envisaged data transfers to a third country, or an international organisation,
- the preservation period,
- the knowledge of the reasoning underlying data processing where the results of such processing are applied to her or him, notably in the case of profiling.

12.2 The data subject has the right to erasure of data concerning him/her processed ~~against~~contrary to the principles of this Recommendation~~is exercised subject to legitimate grounds~~. The data subject is entitled to obtain rectification of data concerning her or him. The data subject furthermore has the right to object on grounds relating to her or his personal situation to the processing of her or his health-related data, unless it is anonymised or the controller demonstrates an overriding and legitimate reason for pursuing the data processing.

12.3 If the request to rectify or erase the data is refused or if the data subject's objection is rejected, he or she should be able to ~~appeal~~have a remedy.

12.4 The data subject has the right ~~The right to data portability enables the data subject to require~~s, subject to conditions prescribed by law, to receive from the controller, where the processing is performed by automatic means, the transmission - in a structured, interoperable and machine-readable format - of her or his personal data with a view to transmitting them to another controller. The data subject has also the right to have his/her personal data ~~can also require from the controller that he or she~~ transmitted~~s~~ directly ~~the data~~ to another controller, ~~,~~ where technically feasible

12.5 The rights of data subjects should be easy to exercise and all States ~~must~~ should ensure that every person is given the necessary and ~~,~~ adequate, ~~legal, effective and practical~~ means to exercise their rights.

12.6 Health professionals have to put in place all necessary measures in order to ensure respect for the effective exercise of such rights as an element of their professional deontology, as recognised by domestic law.

12.7 The rights of data subjects can be subject to restrictions provided for by law, where such restrictions are necessary and proportionate measures in a democratic society for the reasons specified in Article 9 of Convention 108, notably objectives of general public interest of the State relating to public health.

1.10 Chapter IV. ~~Reference frameworks of i~~ Security and interoperability

~~13. Reference frameworks~~

~~13.1 Interoperability of systems enables to contribute to data portability and should for this reason be encouraged. The processing of health-related data furthermore requires that all players observe high standards to ensure the lawfulness of the processing and security and confidentiality of such data. Reference frameworks, offering a technical frame, may facilitate interoperability and security.~~

~~13.2 Reference frameworks should be taken into consideration at the design stage of information systems and compliance with them is of particular importance where health-related data are collected and processed in connection with care and treatment.~~
~~Reference frameworks defined by the stakeholders and based on international norms aim at setting standards enabling the portability, exchange and sharing of health-related data by information systems and at facilitating the monitoring of their implementation under the conditions of security required, for instance through certification schemes.~~

13~~5~~. Security ~~reference frameworks~~

1~~5~~3.1 The processing of health-related data is to be made secure and security ~~policies~~ measures adapted to the risks for fundamental rights and freedoms must in that regard be defined to ensure that all players observe high standards guaranteeing the lawfulness of the processing and security and

Comment [A37]: Maybe redundant. In that case it would not be personal data…

Comment [A38]: The sentence is not clear

Comment [A39]: More than simply "be able to require", the data should have the right to have his data transmitted directly to another controller, where feasible. See GDPR.

confidentiality of such data.

153.2 These security rules, defined by domestic law and possibly contained in reference frameworks, constantly kept state-of-the-art and regularly reviewed, should result in the adoption of ~~such~~ technical and organisational measures as to protect personal health-related data from any illegal or accidental destruction, any loss or any impairment, and to guard against any unauthorised access or unavailability or inaccessibility. In particular, ~~domestic~~ the law should make provision for organising and regulating procedures concerning the collection, storage and restitution of health-related data.

135.3 System availability – i.e. the proper functioning of the system – 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.

135.4 Guaranteeing integrity requires verification of every action carried out on the data, any changes made to or deletion of data, including the communication of data. It also requires the establishment of measures to monitor access to the data base and the data themselves, ensuring that only authorised persons are able to access the data.

135.5 Auditability should lead to a system making it possible to trace any access to the information system and modifications made and for any action carried out, to be able to identify its author.

135.6 Activity entailing hosting health-related data and making them available for users should comply with the ~~security reference framework and~~ principles of personal data protection including those contained in appropriate reference frameworks.

135.7 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-related data. They must have full regard for professional secrecy and comply with appropriate measures laid down in ~~domestic~~ law to guarantee the confidentiality and security of the data.

14. Interoperability ~~reference frameworks~~

~~13. Reference frameworks~~

143.1 Interoperability of systems enables to contribute to data portability and should for this reason be encouraged. ~~The processing of health-related data furthermore requires that all players observe high standards to ensure the lawfulness of the processing and security and confidentiality of such data.~~ Reference frameworks, offering~~ing~~ a technical frame, ~~may~~ facilitating interoperability based on international norms, should ensure that a high level of security is guaranteed while providing for such interoperability. The monitoring of the implementation of reference frameworks can be done through certification schemes ~~and security~~.

~~14.2 Reference frameworks should be taken into consideration at the design stage of information systems.~~

Comment [A40]: Still not convinced about the appropriateness of this sentence. Is it for the T-PD to say that reference framework should be considered at the design stage of information systems?

1.11 Chapter V. Scientific research

156. Scientific research

165.1 The processing of health-related data for the purposes of scientific research should be subject to appropriate safeguards, complementing the other provisions of the present recommendation, and be carried out with a legitimate aim for the rights and fundamental freedoms of the data subject.

165.2 The need to process health-related data for the purposes of scientific research should be evaluated in the light of the aim pursued and the risks to the data subject and, in relation to genetic data to her or his biological family.

1~~6~~5.3 The data subject should, in addition to what is foreseen in Chapter III be provided with prior, transparent and comprehensible information that is as precise as possible with regard to:

- the nature of the envisaged scientific research, the possible choices that he or she could exercise as well as any relevant conditions governing the use of the data, including re-contact and feedback;
- the conditions applicable to the storage of the data, including access and possible communication policies; and
- the rights and safeguards provided for by law, and specifically of her or his right to refuse to participate in the research and withdraw at any time.

Restrictions may be applied in the event of a medical emergency provided that appropriate safeguards are ensured.

1~~6~~5.4 As it is not always possible to determine beforehand the purposes of different research projects at the time of the collection of data, data subjects should be able ~~ ~~to exercise a choice solely for certain ~~fields~~ areas of research or certain parts of research projects, to the extent allowed by the intended purpose, with due regard for recognised ethical standards.

1~~5~~6.5 Health-related data should only be used in a research project if the data subject, after having received prior information according to the provisions of paragraph 1~~5~~6.3, has consented to it or, if permitted by law providing appropriate safeguards, has not objected to it. If the proposed use of the data in a research project is not explained prior to collection of the data, reasonable efforts should be made to contact the data subject. The wish of the data subject not to be contacted should be observed. Where the attempt to contact the data subject proves unsuccessful, the health-related data should only be used in the research project subject to an independent evaluation of the fulfillment of the following conditions:

e. evidence is provided that reasonable efforts have been made to contact the person concerned;

f. the research addresses an overriding scientific interest and the processing is proportionate to the objective pursued ;

g. the aims of the research could not reasonably be achieved without using the data for which consent cannot be obtained; and

h. there is no evidence that the person concerned has expressly opposed such research use.

1~~6~~5.6 The conditions in which health-related data are processed for scientific research must be assessed, where necessary, by the body or bodies designated by ~~domestic~~ law.

1~~6~~5.7 Healthcare professionals who are entitled to carry out their own medical research and scientists in other disciplines should be able to use the health-related data which they hold as long as the data subject has been informed of this possibility beforehand in compliance with paragraph 1~~5~~6.3 and subject to complementary safeguards determined by ~~domestic~~ law such as requiring explicit consent or the assessment of the competent body designated by law.

1~~6~~5.8 Where possible, data should be anonymised and where it is not possible, pseudonymisation of the data, with intervention of a trusted third-party at the separation stage of the identification, is among the measures that should be implemented to safeguard the rights and fundamental freedoms of the data subject. This must be done where the purposes of the scientific research can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects.

1~~6~~5.9 Where a data subject withdraws from a scientific research, her or his health-related data processed in the context of that research should be destroyed or anonymised in a manner not to compromise the scientific validity of the research and the data subject should be informed accordingly.

Comment [A41]: At least in the EM we should recall that in any case the appropriate safeguards should be ensured (see 15.1) as consent cannot be the only requirement to render the processing legitimate.

Comment [A42]: Check consistency with Article 21 of the GDPR which ensures the right to object unless the processing is necessary for reasons of public interest

15~~6~~.10 Personal data used for scientific research should not be published in a form which enables the data subjects to be identified, except where he or she has consented to it and domestic law allows it.

1.12 Chapter VI – Mobile applications

~~Mobile applications enable the development of new practices in the medical and public health fields. They include applications used in our daily lives of « quantified self » connecting to medical devices as well as systems of personal advice and monitoring.~~

16~~7~~. Mobile applications

17~~6~~.1 Where the data collected by these applications, whether implanted on the person or not, may reveal information on the physical or mental state of a person in connexion with her or his health or concern any information regarding health care and medico-social provision, they constitute health-related data. In this connection they enjoy the same legal protection and confidentiality applicable to other health-related data processing as defined by the present Recommendation and, where applicable, supplemented by the domestic law.

17~~6~~.2 Persons using such mobile applications, as soon as they involve the processing of their personal data, must enjoy the same rights as those provided for in Chapter III of the present Recommendation. They must notably have obtained beforehand all necessary information on the nature and functioning of the system in order to be able to control its use. To this effect clear and transparent information on the intended processing should be drafted by the controller with the participation of the software designer and the software distributor whose respective roles have to be determined in advance.

17~~6~~.3 Any use of mobile applications must be accompanied by specific, tailored and state-of-the-art security measures which notably provide for the authentication of the person concerned and the encryption of the transmission of data.

16~~7~~.4 The hosting, by a third party of health-related data produced by mobile applications must obey security rules providing for the confidentiality, integrity and restitution of the data upon request of the data subject.

MEXICO / MEXIQUE

Comments on

DRAFT RECOMMENDATION ON THE PROTECTION OF HEALTH-RELATED DATA

Recommendation

Recommendation CM/Rec(2018)…. of the Committee of Ministers to member States on the protection of health-related data

(adopted by the Committee of Ministers … 2018, at the … meeting of the Ministers' Deputies)

Having regard to the provisions of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 (ETS No. 108, hereinafter the "Convention No. 108") and of its Additional Protocol regarding supervisory authorities and transborder data flows of 8 November 2001 (ETS No. 181), the Committee of Ministers is convinced of the desirability of facilitating the application of those principles to the processing of health-related data.

States face major challenges today, relating to the processing of health-related data, which now takes place in an environment that has changed considerably since the adoption of Recommendation (97)5 on the protection of medical data.

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

The benefits of this increasing digitisation of data can be found in numerous occasions, such as in the enhancement of public health policies, medical treatment or patients' care. The prospects of such benefits require that the advent and never-ending increase of the quantity of data, coupled to the technical analysis capacities linked to personalised health care be accompanied by legal and technical measures enabling an effective protection of every individual.

People's desire to have more control over their personal data and the decisions based on the processing of such data, the increasing involvement of patients in understanding the manner in which decisions concerning them are being taken, are additional features of this change.

Besides, geographical mobility accompanied by the development of medical devices and connected objects is also contributing 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 (97) 5 on the protection of medical data, with the more general term "health-related data" being preferred, while reaffirming the sensitivity of health-related data and the importance of regulating their use so as to guarantee due regard for the rights and fundamental freedoms of every individual, in particular the right to protection of privacy and personal data.

Health-related data are among the data belonging to a special category which, under Article 6 of Convention 108, enjoy a higher level of protection due notably to the risk of discrimination which may occur with their processing.

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

The processing of health-related data shall always aim serving the data subject and at enhancing the quality and efficiency of care, possibly also enhancing health systems, while respecting individuals fundamental rights.

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 (97) 5 mentioned above, are reflected in their law and practice;

- ensure, to that end, that the present Recommendation and its appendix are brought to the attention of the authorities responsible for healthcare systems, with the latter being responsible for promoting their transmission to the various actors who process health-related data, in particular healthcare professionals, data protection officers or persons having similar duties;

- 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 players who process health-related data and taken into account in the design, deployment and use of the information and communication technologies (ICTs) in that sector.

***

Appendix to Recommendation CM/Rec(2018)…

1.13 Chapter I. General provisions

1. Purpose

The purpose of this Recommendation is to provide member States with guidance for regulating the processing of health-related data in order to guarantee respect for the rights and fundamental freedoms of every individual, particularly the right to privacy and to protection of personal data as required by Article 8 of the European Convention on Human Rights. It also highlights to this end the importance of developing secured interoperable information systems in a manner enabling the enhancement of efficient and secured health systems.

2. Scope

This Recommendation is applicable to the processing of personal data relating to health in the public and private sectors. To this end, it also applies to the exchange and sharing of health-related data by means of digital tools. It should not be interpreted as limiting or otherwise affecting the possibility for ~~domestic~~ law to grant data subjects a wider measure of protection~~.~~, as well as that the member states are obliged to modify their legislation on the matter for the fulfilment of this recommendation.

Comment [A43]: INAI's Suggestion

~~To this end, it also applies to the exchange and sharing of health-related data by means of digital tools. Such tools should be designed to ensure respect for the rights and fundamental freedoms of individuals.~~

The provisions of this Recommendation do not apply to health-related data processing performed by individuals in the context of purely personal or household 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 ("data subject"). An individual shall not be regarded as "identifiable" if identification requires unreasonable time, effort or resources.

- The expression "data processing" means any operation or set of operations which is performed on

personal data, such as the collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure, or destruction of, or the carrying out of logical and/or arithmetical operations on such data.

- The expression “anonymisation” refers to the process applied to personal data so that the data subjects can no longer be identified either directly or indirectly.

- The expression “pseudonymisation” refers to a type of processing ~~which makes it possible to process~~ in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information kept separately and subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable individual. Pseudonymised data are personal data.

- The expression “health-related data” means all personal data concerning the physical or mental health of an individual, including the provision of healthcare services, which reveals information about this person’s past, current and future health.

- The expression “genetic data” means all data relating to the genetic characteristics of an individual which have been either inherited or acquired during early prenatal development, as they result from an analysis of a biological sample from the individual concerned: chromosomal, DNA or RNA analysis or analysis of any other element enabling equivalent information to be obtained.

~~- The expression “data processing” means any operation or set of operations which is performed on personal data, such as the collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure, or destruction of, or the carrying out of logical and/or arithmetical operations on such data.~~

- The expression “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 expression “processor” means a natural or legal person, public authority, service, agency or any other body which processes data on behalf of the controller.

- The expression "reference framework" denotes a coordinated set of rules and/or processes kept constantly state-of-the-art, adapted to practice and applicable to health information systems, covering the areas of interoperability and security. Such frameworks may be given a binding nature by domestic law.

- The expression "mobile applications" denotes a set of means accessible in a mobile environment making it possible to communicate and manage health-related data remotely. It covers different forms such as connected medical objects and devices which can be used for diagnostic, treatment or wellbeing purposes among other things.

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

- The expression "data hosting" denotes the use of external data service providers irrespective of the platform used for the secure and lasting digital storage of data.

1.14 Chapter II. The legal conditions for the processing of health-related data

4. Principles concerning data processing

4.1 Anyone processing health-related data should comply with the following principles:

a. the data must be processed in a tran**sparent, lawful and fair manner**.

b. the data must be collected for explicit, specific and legitimate purposes as prescribed in principle 5 and must not be processed in a manner which is incompatible with these purposes. Further processing for archiving purposes in the public interest, for scientific or historical research purposes

Comment [A44]: It is suggested to use the terms "among others" or "without limitation", with the purpose of not limiting the type of operations carried out with personal data

or statistical purposes is not regarded as incompatible with the initial purposes, where appropriate guarantees enable rights and fundamental freedoms to be respected.

c. The processing of data should be proportionate in relation to the legitimate purpose pursued and shall be carried out only on the basis of consent of the data subject as laid down in principle 5.2 or on other legitimate basis as laid down in other paragraphs of principle 5.

d. Personal data should, in principle and as far as possible, be collected from the data subject. Where the data subject is not in a capacity to provide the data and such data are necessary for the purposes of the processing, they can be collected from other sources in accordance with the principles of this recommendation.

e. The data must be adequate, relevant and not excessive in relation to the purposes for which they are processed; they must be accurate and, if necessary, kept up to date.

f. Appropriate security measures, taking into consideration the latest technological developments, the sensitive nature of health-related data, the security breaches occurred and the assessment of potential risks, should be established to prevent risks such as accidental or unauthorised access to, destruction, loss, use, unavailability, inaccessibility, modification or disclosure of personal data.

Comment [A45]: INAI's Suggestion

Health-related data must be cancelled once the purposes that motivated its treatment are fulfilled, through the application of policies, methods and techniques aimed at the definitive suppression of them, in such way that the probability of recovering or reusing them is minimal.

Comment [A46]: INAI's Suggestions

g. The rights of the person whose data are processed must be respected, particularly the rights of access to the data, information, rectification, objection, deletion and portability as prescribed in principle 12 of the present recommendation.

4.2 Personal data protection principles must be taken into account by default and incorporated right from the design of information systems which process health-related data. Compliance with these principles should be regularly reviewed throughout the life cycle of the processing (privacy by design). The controller should carry out, before commencing the processing and at regular intervals, an assessment of the potential impact of the processing of data foreseen in terms of data protection and respect for privacy.

4.3 Data controllers and the processors acting under their responsibility should take all appropriate measures to fulfil their obligations with regard to data protection and should be able to demonstrate in particular to the competent supervisory authority that the processing is in line with those obligations.

4.4 Data controllers and their processors who are not health professionals should only process health-related data in accordance with rules of confidentiality and security measures, as well as the functions they perform, that ensure a level of protection equivalent to the one imposed to health professionals.

Comment [A47]: INAI's Suggestion

5. ~~Purposes and l~~Legitimate basis of health-related data processing

5.1 Health-related data may only be processed where appropriate safeguards are enshrined in law and ~~provided and~~ the processing is necessary ~~for one of the following purposes~~for:

p. ~~for~~ preventive medical purposes and ~~for~~ purposes of medical diagnosis, administration of care or treatment, or management of health services by health professionals and those of the social and medico-social sector, subject to the conditions defined by ~~domestic~~ law;

q. ~~for~~ reasons of public health, such as for example protection against health hazards, humanitarian action or in order to ensure a high standard of quality and safety for medical treatment, health products and medical devices, subject to the conditions defined by ~~domestic~~ law;

r. ~~for~~ the purpose of safeguarding the vital interests of the data subject or of another person where consent cannot be collected;

s. ~~for~~ reasons of public interest in the field of managing claims for social welfare and health insurance benefits and services, subject to the conditions defined by ~~domestic~~ law;

~~t. [for reasons of public health compatible with the initial purpose of the collection of data, provided that they are lawful and legitimate, subject to the conditions defined by domestic law;]~~

~~u.~~t. ~~for~~ processing for archiving purposes in the public interest, for scientific or historical research purposes or statistical purposes subject to the conditions defined by ~~domestic~~ law (such as for instance the obligation of prior information of the data subject to enable the exercise of the right to refuse participation in a scientific research) in order to guarantee protection of the data subject's fundamental rights and legitimate interests;

~~v.~~u. ~~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~~ law or any collective agreement complying with the said law;

~~w.~~v. ~~for~~ reasons essential to the recognition, exercise or defence of a legal claim.

5.2 Health-related data may also be processed if the data subject has given her or his consent, except in cases where domestic law provides that a ban on health-related data processing cannot be lifted solely by the data subject's consent. Where consent of the data subject to the processing of health-related data is required, in accordance with domestic law, it should be free, specific, informed and explicit. Consent can be expressed by electronic means.

5.3 Health-related data may also be processed where the processing is necessary for the execution~~based on~~ of a contract entered into by the data subject or on his or her behalf with a health professional subject to conditions defined by law, including the obligation of secrecy.

5.4 In all cases, appropriate safeguards should be established in order to guarantee, in particular, the security of the 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 unborn children

Health-related data concerning unborn children, inter alia such as data resulting from a prenatal diagnosis or from the identification of the genetic characteristics of such children should enjoy an appropriate protection.

7. Genetic data

7.1 Genetic data should only be collected subject to appropriate safeguards and where it is either prescribed by law~~,~~ or on the basis of the consent expressed by the data subject, except where consent is excluded by law as legal basis for the processing of genetic data. ~~where this is required by law, and subject to appropriate safeguards~~.

7.2 Genetic data processed with a preventive aim, for diagnosis or for treatment of the data subject or a member of her or his biological family or for scientific research should be used only for these purposes or to enable the persons concerned by the results of such tests to take an informed decision on these matters.

7.3 Processing of genetic data for the purpose of a judicial procedure or investigation should be used only when there are no alternative or less intrusive means to establish whether there is a genetic link in the context of the production of evidence, to prevent a real and immediate danger or to for the prosecution of a specific criminal offence. Such data should not be used to determine other characteristics which may be linked genetically, except where domestic law provides for it with appropriate safeguards.

7.4 Any processing of genetic data prescribed by law other than in the cases provided for in paragraphs 7.2 and 7.3 should only be carried out to avoid any serious prejudice to the health of the data subject or of a member of her or his biological family or for reasons in relation with humanitarian action.

7.5 Existing predictive data resulting from genetic tests should not be processed for insurance purposes, except where this is specifically provided for by law. In that case, their processing should only be authorised in full respect of the applicable criteria defined by law, in light of the type of test used and the particular risk concerned. The provisions of Recommendation (2016)8 on the processing of personal health-related data for insurance purposes, including data resulting from genetic tests are also to be taken into consideration in that regard.

7.6 The data subject is entitled to know any information collected about her or his health. However, the wish of the person whose genetic data are analysed not to know should be taken into consideration, and that person should be informed, prior to such analysis, of the possibility of not being informed of the results, including of unexpected findings. Her or his wish not to know may, in her or his interests or in the interests of a member of her or his biologic family, have to be restricted as foreseen by law, notably in light of the doctors' duty to provide care.

~~7.7 The publication of genetic data which would identify the data subject or a person who has a direct link with her or his genetic line, should be prohibited, except where the data subject has expressly consented beforehand to it and it is prescribed by law, for specific purposes and with the appropriate safeguards.~~

8. Shar**ing of health-related data** ~~**ed professional secrecy**~~ **for purposes of providing and administering health care**

8.1 Where health-related data are shared by different professionals for purposes of providing and administering health care of an individual, the data subject ~~should~~ shall be informed beforehand, except where this proves to be impossible due to an emergency, of the nature of the health-related data processed and of the health professionals participating in the provision of care. The data subject must be able, in accordance with safeguards prescribed by law, to withdraw consent, where such consent is required by law, or object at any time to the exchange and sharing of her or his health-related data.

8.2 ~~In the interests of greater co-ordination between p~~Professionals operating on a particular individual case in the health and medico-social sector and sharing data in the interests of greater co-ordination should be subject to professional confidentiality incumbent upon a health-care professional, or to equal rules of confidentiality~~, the domestic law 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 should be limited to the information strictly necessary for the co-ordination or continuity of care, prevention or medico-social and social follow-up of the individual, with the respective actors only able in this case to share or receive data lying strictly within the scope of their tasks and depending on their authorisations. Appropriate measures should be taken to ensure the security of the data.

8.4 The use of an electronic medical file and of an electronic mailbox allowing for the sharing and exchange of health-related data should respect those principles.

In the exchange of health-related data, physical, technical and administrative security measures should be adopted, as well as those necessary to guarantee the confidentiality, integrity and availability of health-related data.

Comment [A48]: INAI's suggestion

9. Communication ~~to 'authorised recipients'~~ of health-related data

9.1 Health-related data may be communicated to recipients where the latter are authorised by ~~domestic~~ law to have access to the data. ~~Such authorised recipients may be judicial authorities, experts appointed by a court authority, members of staff of an administrative authority designated by a legal formal act or humanitarian organisations, among other people.~~

9.2 ~~Medical officers of i~~Insurance companies and employers cannot, in principle, be regarded as recipients authorised to have access to the health-related data of patients unless domestic law makes provision for this with appropriate safeguards and if the data subject has validly consented to it.

9.3 Health-related data will, unless other appropriate safeguards are provided for by ~~domestic~~ law, only be communicated to an authorised recipient who is subject to the rules of confidentiality incumbent upon a health-care professional, or to equal rules of confidentiality.

10. Storage of health-related data

The data should not be stored in a form which permits identification of the data subjects for longer than is necessary for the purposes for which they are processed unless they are used for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes and where appropriate measures enable to safeguard the rights and fundamental freedoms of the data subject. In this case, data should in principle be anonymised as soon as the research, the archiving activity or the statistical study enables it.

1.15 Chapter III. The rights of the data subject

11. Transparency of processing

11.1 The data subject must be informed by the controller of the processing of their health-related data.

The information must include:

- 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,
- the length of ~~conservation~~ preservation of the data,
- the recipients or categories of recipients of the data, and planned data transfers to a third country, or an international organisation,
- the possibility, if applicable, of objecting to the processing of their data, in the conditions prescribed in paragraph 12.2,
- the conditions and the means made available to them for exercising via the controller their rights of access, the right of rectification and the right to erasure of their health-related data.

The information must where necessary, with a view to ensuring a fair and transparent processing, also include:

- that their data may subsequently be processed for a compatible purpose, in accordance with appropriate safeguards provided for by domestic law and in the conditions prescribed in paragraph 4.1.b,
- the specific techniques used to process their health-related data,
- the possibility of lodging a complaint with a supervisory authority,
- the existence of automated decisions, including profiling ~~where~~ which is only permissible where prescribed by~~domestic~~ law ~~allows~~ and~~it~~ subject to appropriate safeguards.

11.2 This information should be provided prior to data collection or at the first communication, unless it proves impossible or requires disproportionate efforts from the controller, in particular for processing for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes.

11.3 The information must be intelligible and easily accessible, in a clear and plain language and suited to the circumstances to allow a full understanding of the processing by the data subject. In particular, where the data subject is physically or legally incapable of receiving the information, it may be given to the person legally representing her or him. If a legally incapacitated person is capable of understanding, he or she should be informed before the data are processed.

11.4 Only urgency or the impossibility for the data subject to be informed can give rise to an exemption from the obligation of informing. In such a case, information should be provided as soon as possible.

11.5 A person's wish to be kept in ignorance of a diagnosis or prognosis should be complied with, except where this constitutes a serious risk for the health of third parties.

11.6 Domestic law should provide for appropriate safeguards ensuring respect for these rights.

12. The rights of access, objection, rectification, erasure and data portability

12.1 The data subject has the right to know whether personal data which concern her or him are being processed, and, if so, to obtain - without excessive delay or expense and in an intelligible form - communication of her or his data and to have access~~, without excessive delay or expense and in an intelligible form,~~ in the same conditions to at least the following information:

- the purpose or purposes of the processing,
- the categories of personal data concerned,
- the recipients or categories of the recipients of the data and the envisaged data transfers to a third country, or an international organisation,
- the preservation period,
- the knowledge of the reasoning underlying data processing where the results of such processing are applied to her or him, notably in the case of profiling.

12.2 The data subject has the right to erasure of data processed against the principles of this Recommendation~~is exercised subject to legitimate grounds~~. The data subject is entitled to obtain rectification of data concerning her or him. The data subject furthermore has the right to object on grounds relating to her or his personal situation to the processing of her or his health-related data, unless it is anonymised or the controller demonstrates an overriding and legitimate reason for pursuing the data processing.

12.3 If the request to rectify or erase the data is refused or if the data subject's objection is rejected, he or she should be able to ~~appeal~~have a remedy.

12.4 The right to data portability ~~enables the data subject to~~ requires, subject to conditions prescribed by law, from the controller, where the processing is performed by automatic means, the transmission - in a structured, interoperable and machine-readable format - of her or his personal data with a view to transmitting them to another controller. The data subject can also require from the controller that he or she transmits directly the data to another controller.

The data subject has the right to request a copy of their personal data in a structured, interoperable and machine readable format that allows the reuse and / or use of personal data.

Comment [A49]: INAI's suggestion

12.5 The rights of data subjects should be easy to exercise and all States ~~must~~ should ensure that every person is given the necessary and ~~,~~ adequate, ~~legal, effective and practical~~ means to exercise their rights.

12.6 Health professionals have to put in place all necessary measures in order to ensure respect for the effective exercise of such rights as an element of their professional deontology, as recognised by domestic law.

12.7 The rights of data subjects can be subject to restrictions provided for by law, where such restrictions are necessary and proportionate measures in a democratic society for the reasons specified in Article 9 of Convention 108, notably objectives of general public interest of the State

relating to public health.

1.16 Chapter IV. ~~Reference frameworks of i~~ Security and interoperability

~~**13. Reference frameworks**~~

~~13.1 Interoperability of systems enables to contribute to data portability and should for this reason be encouraged. The processing of health-related data furthermore requires that all players observe high standards to ensure the lawfulness of the processing and security and confidentiality of such data. Reference frameworks, offering a technical frame, may facilitate interoperability and security.~~

~~13.2 Reference frameworks should be taken into consideration at the design stage of information systems and compliance with them is of particular importance where health-related data are collected and processed in connection with care and treatment.~~
~~Reference frameworks defined by the stakeholders and based on international norms aim at setting standards enabling the portability, exchange and sharing of health related data by information systems and at facilitating the monitoring of their implementation under the conditions of security required, for instance through certification schemes.~~

13~~5~~. Security ~~reference frameworks~~

1~~5~~3.1 The processing of health-related data is to be made secure and security ~~policies~~ measures adapted to the risks for fundamental rights and freedoms must in that regard be defined to ensure that all players observe high standards guaranteeing the lawfulness of the processing and security and confidentiality of such data.

1~~5~~3.2 These security rules, defined by domestic law and possibly contained in reference frameworks, constantly kept state-of-the-art and regularly reviewed, should result in the adoption of ~~such~~ technical and organisational measures as to protect personal health-related data from any illegal or accidental destruction, any loss or any impairment, and to guard against any unauthorised access or unavailability or inaccessibility. In particular, ~~domestic~~ the law should make provision for organising and regulating procedures concerning the collection, storage and restitution of health-related data.

13~~5~~.3 System availability – i.e. the proper functioning of the system – 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.

13~~5~~.4 Guaranteeing integrity requires verification of every action carried out on the data, any changes made to or deletion of data, including the communication of data. It also requires the establishment of measures to monitor access to the data base and the data themselves, ensuring that only authorised persons are able to access the data.

13~~5~~.5 Auditability should lead to a system making it possible to trace any access to the information system and modifications made and for any action carried out, to be able to identify its author.

13~~5~~.6 Activity entailing hosting health-related data and making them available for users should comply with the security reference framework and principles of personal data protection.

13~~5~~.7 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-related data. They must have full regard for professional secrecy and comply with appropriate measures laid down in ~~domestic~~ law to guarantee the confidentiality and security of the data.

The data controller must inform about the health-related data breaches that occurred at any stage of their treatment, in accordance with the national legislation on the protection of personal data.

14. Interoperability ~~reference frameworks~~

~~**13. Reference frameworks**~~

143.1 Interoperability of systems enables to contribute to data portability and should for this reason be encouraged. ~~The processing of health-related data furthermore requires that all players observe high standards to ensure the lawfulness of the processing and security and confidentiality of such data.~~ Reference frameworks, offering~~ing~~ a technical frame,~~ may~~ facilitating~~e~~ interoperability based on international norms should ensure that a high level of security is guaranteed while providing for such interoperability. The monitoring of the implementation of reference frameworks can be done through certification schemes~~ and security~~.

14.2 The national legislation that is applicable to member states as a Reference frameworks should be taken into consideration at the design stage of information systems.

Comment [A50]: INAI's suggestion

1.17 Chapter V. Scientific research

15~~6~~. Scientific research

16~~5~~.1 The processing of health-related data for the purposes of scientific research should be subject to appropriate safeguards, complementing the other provisions of the present recommendation, and be carried out with a legitimate aim for the rights and fundamental freedoms of the data subject.

16~~5~~.2 The need to process health-related data for the purposes of scientific research should be evaluated in the light of the aim pursued and the risks to the data subject and, in relation to genetic data to her or his biological family.

16~~5~~.3 The data subject should, in addition to what is foreseen in Chapter III be provided with prior, transparent and comprehensible information that is as precise as possible with regard to:

- the nature of the envisaged scientific research, the possible choices that he or she could exercise as well as any relevant conditions governing the use of the data, including re-contact and feedback;
- the conditions applicable to the storage of the data, including access and possible communication policies; and
- the rights and safeguards provided for by law, and specifically of her or his right to refuse to participate in the research and withdraw at any time.

Restrictions may be applied in the event of a medical emergency provided that appropriate safeguards are ensured.

16~~5~~.4 As it is not always possible to determine beforehand the purposes of different research projects at the time of the collection of data, data subjects should be able ~~–~~to exercise a choice solely for certain ~~fields~~ areas of research or certain parts of research projects, to the extent allowed by the intended purpose, with due regard for recognised ethical standards.

15~~6~~.5 Health-related data should only be used in a research project if the data subject, after having received prior information according to the provisions of paragraph 15~~6~~.3, has consented to it or, if permitted by law providing appropriate safeguards, has not objected to it. If the proposed use of the data in a research project is not explained prior to collection of the data, reasonable efforts should be made to contact the data subject. The wish of the data subject not to be contacted should be observed. Where the attempt to contact the data subject proves unsuccessful, the health-related data should only be used in the research project subject to an independent evaluation of the fulfillment of the following conditions:

i. evidence is provided that reasonable efforts have been made to contact the person concerned;

j. the research addresses an overriding scientific interest and the processing is proportionate to the objective pursued ;

k. the aims of the research could not reasonably be achieved without using the data for which consent cannot be obtained; and

l. there is no evidence that the person concerned has expressly opposed such research use.

16~~5~~.6 The conditions in which health-related data are processed for scientific research must be assessed, where necessary, by the body or bodies designated by ~~domestic~~ law.

16~~5~~.7 Healthcare professionals who are entitled to carry out their own medical research and scientists in other disciplines should be able to use the health-related data which they hold as long as the data subject has been informed of this possibility beforehand in compliance with paragraph 15~~6~~.3 and subject to complementary safeguards determined by ~~domestic~~ law such as requiring explicit consent or the assessment of the competent body designated by law.

16~~5~~.8 Where possible, data should be anonymised and where it is not possible, pseudonymisation of the data, with intervention of a trusted third-party at the separation stage of the identification, is among the measures that should be implemented to safeguard the rights and fundamental freedoms of the data subject. This must be done where the purposes of the scientific research can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects.

16~~5~~.9 Where a data subject withdraws from a scientific research, her or his health-related data processed in the context of that research should be destroyed or anonymised in a manner not to compromise the scientific validity of the research and the data subject should be informed accordingly.

15~~6~~.10 Personal data used for scientific research should not be published in a form which enables the data subjects to be identified, except where he or she has consented to it and domestic law allows it.

1.18 Chapter VI – Mobile applications

~~Mobile applications enable the development of new practices in the medical and public health fields. They include applications used in our daily lives of « quantified-self » connecting to medical devices as well as systems of personal advice and monitoring.~~

16~~7~~. Mobile applications

17~~6~~.1 Where the data collected by these applications, whether implanted on the person or not, may reveal information on the physical or mental state of a person in connexion with her or his health or concern any information regarding health care and medico-social provision, they constitute health-related data. In this connection they enjoy the same legal protection and confidentiality applicable to other health-related data processing as defined by the present Recommendation and, where applicable, supplemented by the domestic law.

During the design and development of these applications, mechanisms and controls must be incorporated to comply with the national legislation on personal data protection.

Comment [A51]: INAI's suggestion

17~~6~~.2 Persons using such mobile applications, as soon as they involve the processing of their personal data, must enjoy the same rights as those provided for in Chapter III of the present Recommendation. They must notably have obtained beforehand all necessary information on the nature and functioning of the system in order to be able to control its use. To this effect clear and transparent information on the intended processing should be drafted by the controller with the participation of the software designer and the software distributor whose respective roles have to be determined in advance.

17~~6~~.3 Any use of mobile applications must be accompanied by specific, tailored and state-of-the-art security measures which notably provide for the authentication of the person concerned and the encryption of the transmission of data.

16~~7~~.4 The hosting, by a third party of health-related data produced by mobile applications must obey security rules providing for the confidentiality, integrity and restitution of the data upon request of the data subject.

EUROPEAN DATA PROTECTION SUPERVISOR (EDPS) / LE CONTRÔLEUR EUROPEEN DE LA PROTECTION DES DONNÉES (CEPD)

Recommendation

Recommendation CM/Rec(2018)…. of the Committee of Ministers to member States on the protection of health-related data

(adopted by the Committee of Ministers … 2018, at the … meeting of the Ministers' Deputies)

Having regard to the provisions of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 (ETS No. 108, hereinafter the "Convention No. 108") and of its Additional Protocol regarding supervisory authorities and transborder data flows of 8 November 2001 (ETS No. 181), the Committee of Ministers is convinced of the desirability of facilitating the application of those principles to the processing of health-related data.

States face major challenges today, relating to the processing of health-related data, which now takes place in an environment that has changed considerably since the adoption of Recommendation (97)5 on the protection of medical data.

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

The benefits of this increasing digitisation of data can be found in numerous occasions, such as in the enhancement of public health policies, medical treatment or patients' care. The prospects of such benefits require that the advent and never-ending increase of the quantity of data, coupled to the technical analysis capacities linked to personalised health care be accompanied by legal and technical measures enabling an effective protection of every individual.

People's desire to have more control over their personal data and the decisions based on the processing of such data, the increasing involvement of patients in understanding the manner in which decisions concerning them are being taken, are additional features of this change.

Besides, geographical mobility accompanied by the development of mobile health applications, medical devices and connected objects is also contributing to new uses and to the production of a rapidly growing volume of health-related data, controlled by more diverse stakeholders.

This assessment shared by the member States has prompted to propose a revision of Recommendation (97) 5 on the protection of medical data, with the more general term "health-related data" being preferred, while reaffirming the sensitivity of health-related data and the importance of regulating their use so as to guarantee due regard for the rights and fundamental freedoms of every individual, in particular the right to protection of privacy and personal data.

Health-related data are among the data belonging to a special category which, under Article 6 of Convention No. 108, enjoy a higher level of protection due notably to the risk of discrimination which may occur with their processing.

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

The processing of health-related data shall always aim serving the data subject ~~and~~ or at enhancing the quality and efficiency of care, possibly also enhancing health systems, while respecting individuals fundamental rights.

Comment [A52]: "always serve the data subject" reflect a very individualistic approach to the processing of health-related data. The objective of "enhancing health system" may sometimes contravene certain data subject's interests. I suggest "or" to solve this possible contradiction and include both individualistic and collective interests in health-related processing activities.

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 (97) 5 mentioned above, are reflected in their law and practice;

- ensure, to that end, that the present Recommendation and its appendix are brought to the attention of the authorities responsible for healthcare systems, with the latter being responsible for promoting their transmission to the various actors who process health-related data, in particular healthcare professionals, data protection officers or persons having similar duties;

- 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 players who process health-related data and taken into account in the design, deployment and use of the information and communication technologies (ICTs) in that sector.

Appendix to Recommendation CM/Rec(2018)…

1.19 Chapter I. General provisions

1. Purpose

The purpose of this Recommendation is to provide member States with guidance for regulating the processing of health-related data in order to guarantee respect for the rights and fundamental freedoms of every individual, particularly the right to privacy and to protection of personal data as required by Article 8 of the European Convention on Human Rights. It also highlights to this end the importance of developing secured interoperable information systems in a manner enabling the enhancement of efficient and secured health systems.

2. Scope

This Recommendation is applicable to the processing of personal data relating to health in the public and private sectors. To this end, it also applies to the exchange and sharing of health-related data by means of digital tools. It should not be interpreted as limiting or otherwise affecting the possibility for ~~domestic~~ law to grant data subjects a wider ~~measure of~~ protection.

~~To this end, it also applies to the exchange and sharing of health-related data by means of digital tools. Such tools should be designed to ensure respect for the rights and fundamental freedoms of individuals.~~

The provisions of this Recommendation do not apply to health-related data processing performed by individuals in the context of purely personal or household 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 (“data subject”). An individual shall not be regarded as “identifiable” if identification requires unreasonable time, effort or resources.

- The expression “data processing” means any operation or set of operations which is performed on personal data, such as the collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure, or destruction of, or the carrying out of logical and/or arithmetical operations on such data.

- The expression “anonymisation” refers to the process applied to personal data so that the data subjects can no longer be identified either directly or indirectly.

- The expression “pseudonymisation” refers to a type of processing ~~which makes it possible to process~~ in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information kept separately and subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable individual. Pseudonymised data are personal data.

- The expression “health-related data” means all personal data concerning the physical or mental health of an individual, including the provision of healthcare services, which reveals information about this person’s past, current and future health.

- The expression “genetic data” means all data relating to the genetic characteristics of an individual which have been either inherited or acquired during early prenatal development, as they result from an analysis of a biological sample from the individual concerned: chromosomal, DNA or RNA analysis or analysis of any other element enabling equivalent information to be obtained.

~~- The expression “data processing” means any operation or set of operations which is performed on personal data, such as the collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure, or destruction of, or the carrying out of logical and/or arithmetical operations on such data.~~

- The expression “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 expression “processor” means a natural or legal person, public authority, service, agency or any other body which processes data on behalf of the controller.

- The expression "reference framework" denotes a coordinated set of rules and/or processes kept constantly state-of-the-art, adapted to practice and applicable to health information systems, covering the areas of interoperability and security. Such frameworks may be given a binding nature by domestic law.

- The expression "mobile applications" denotes a set of means accessible in a mobile environment making it possible to communicate and manage health-related data remotely. It covers different forms such as connected medical objects and devices which can be used for diagnostic, treatment or wellbeing purposes among other things.

- The expression “health professionals” covers all professionals recognised as such by domestic law practising in the health, medical welfare or social welfare sector, bound by a confidentiality obligation and involved in ~~co-ordinating treatment for an individual to whom they~~ providinge health care.

- The expression "data hosting" denotes the use of external data service providers irrespective of the platform used for the secure and lasting digital storage of data.

1.20 Chapter II. The legal conditions for the processing of health-related data

4. Principles concerning data processing

4.1 Anyone processing health-related data should comply with the following principles:

a. the data must be processed in a tran**sparent, lawful and fair manner**.

b. the data must be collected for explicit, specific and legitimate purposes as prescribed in principle 5.1 and must not be processed in a manner which is incompatible with these purposes. Further processing for archiving purposes in the public interest, for scientific or historical research purposes or statistical purposes is not regarded as incompatible with the initial purposes, where appropriate guarantees enable rights and fundamental freedoms to be respected.

c. The processing of data should be proportionate in relation to the legitimate purpose pursued and

Comment [A53]: Here I am afraid that the reference to the co-ordination role might be misinterpreted and is restrictive. I suggest to simplify the wording as proposed.

Comment [A54]: I am not sure this definition really brings an added value (the word hosting is only used in 13.6 and 16.4 and the paragraphs may be easily understood without this definition) Moreover, do you envisage only external and digital storage of data (and consider that internal storage or hard copy storage is not data hosting)?

shall be carried out only on the basis of consent of the data subject as laid down in principle 5.2 or on other legitimate basis as laid down in other paragraphs of principle 5.

d. Personal data should, in principle and as far as possible, be collected from the data subject. Where the data subject is not in a capacity to provide the data and such data are necessary for the purposes of the processing, they can be collected from other sources in accordance with the principles of this recommendation.

e. The data must be adequate, relevant and not excessive in relation to the purposes for which they are processed; they must be accurate and, if necessary, kept up to date.

f. Appropriate security measures, taking into consideration the latest technological developments, the sensitive nature of health-related data and the assessment of potential risks, should be established to prevent risks such as accidental or unauthorised access to, destruction, loss, use, unavailability, inaccessibility, modification or disclosure of personal data.

g. The rights of the person whose data are processed must be respected, particularly the rights of access to the data, information, rectification, objection, deletion and portability as prescribed in principle 12 of the present recommendation.

4.2 Personal data protection principles must be taken into account by default and incorporated right from the design of information systems which process health-related data. Compliance with these principles should be regularly reviewed throughout the life cycle of the processing (privacy by design). The controller should carry out, before commencing the processing and at regular intervals, an assessment of the potential impact of the processing of data foreseen in terms of data protection and respect for privacy.

4.3 Data controllers and ~~the~~ processors acting under their responsibility should take all appropriate measures to fulfil their obligations with regard to data protection and should be able to demonstrate in particular to the competent supervisory authority that the processing is in line with those obligations.

4.4 Data controllers and their processors who are not health professionals should only process health-related data in accordance with rules of confidentiality and security measures that ensure a level of protection equivalent to the one imposed to health professionals.

5. ~~Purposes and l~~Legitimate basis~~L~~awfulness of health-related data processing

5.1 Health-related data may only be processed where appropriate safeguards are enshrined in law and ~~provided and~~ the processing is necessary ~~for one of the following purposes~~for:

~~x.~~w. ~~for~~ preventive medical purposes and ~~for~~ purposes of medical diagnosis, administration of care or treatment, or management of health services by health professionals and those of the social and medico-social sector, subject to the conditions defined by ~~domestic~~ law;

~~y.~~x. ~~for~~ reasons of public health, such as for example protection against health hazards, humanitarian action or in order to ensure a high standard of quality and safety for medical treatment, health products and medical devices, subject to the conditions defined by ~~domestic~~ law;

~~z.~~y. ~~for~~ the purpose of safeguarding the vital interests of the data subject or of another person where consent cannot be collected;

~~aa.~~z. ~~for~~ reasons of public interest in the field of managing claims for social welfare and health insurance benefits and services, subject to the conditions defined by ~~domestic~~ law;

~~bb. [for reasons of public health compatible with the initial purpose of the collection of data, provided that they are lawful and legitimate, subject to the conditions defined by~~

Comment [A55]: The Recom uses "should" almost everywhere.

Comment [A56]: Here I still have the feeling that there is no clear distinction between purposes and legitimate bases. It gives the feeling that 5.1 is about the purposes and that 5.2 and 5.3 detail the two only legitimate bases (consent and contract).

During the plenary, the idea was to introduce an introductory paragraph to explain the articulation between the paragraphs, ie controllers or processors may rely on 5.1 **or** on 5.2 **or** on 5.3.

Alternatively, one might merge the paragraphs and the wording could be as follows:

"Health-related data may only be processed where appropriate safeguards are enshrined in law and where :
a. the data subject has given his or her consent ;
b. the processing is necessary for the execution of a contract...
c. the processing is necessary for preventive medical purposes and for purposes of medical diagnosis (...);
d. the processing is necessary for reasons of public health (....)
(....)

~~domestic law;]~~

~~cc.~~aa. ~~for~~ processing for archiving purposes in the public interest, for scientific or historical research purposes or statistical purposes subject to the conditions defined by ~~domestic~~ law (such as for instance the obligation of prior information of the data subject to enable the exercise of the right to refuse participation in a scientific research) in order to guarantee protection of the data subject's fundamental rights and legitimate interests;

~~dd.~~bb. ~~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~~ law or any collective agreement complying with the said law;

~~ee.~~cc. ~~for~~ reasons essential to the recognition, exercise or defence of a legal claim.

5.2 Health-related data may also be processed if the data subject has given her or his consent, except in cases where domestic law provides that a ban on health-related data processing cannot be lifted solely by the data subject's consent. Where consent of the data subject to the processing of health-related data is required, in accordance with domestic law, it should be free, specific, informed and explicit. Consent can be expressed by electronic means.

5.3 Health-related data may also be processed where the processing is necessary for the execution~~based on~~ of a contract for health related purposes entered into by the data subject or on his or her behalf with a health professional subject to conditions defined by law, including the obligation of secrecy.

5.4 In all cases, appropriate safeguards should be established in order to guarantee, in particular, the security of the 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 unborn children

Health-related data concerning unborn children, inter alia such as data resulting from a prenatal diagnosis or from the identification of the genetic characteristics of such children should enjoy an appropriate protection.

7. Genetic data

7.1 Genetic data should only be collected subject to appropriate safeguards and where it is either prescribed by law~~,~~ or on the basis of the valid consent expressed by the data subject, except where consent is excluded by law as legal basis for the processing of genetic data. ~~where this is required by law, and subject to appropriate safeguards~~.

7.2 Genetic data processed with a preventive aim, for diagnosis or for treatment of the data subject or a member of her or his biological family or for scientific research should be used only for these purposes or to enable the persons concerned by the results of such tests to take an informed decision on these matters.

7.3 Processing of genetic data for the purpose of a judicial procedure or investigation should be used only when there are no alternative or less intrusive means to establish whether there is a genetic link in the context of the production of evidence, to prevent a real and immediate danger or ~~to~~ for the prosecution of a specific criminal offence. Such data should not be used to determine other characteristics which may be linked genetically, except where domestic law provides for it with appropriate safeguards.

Comment [A57]: This is an extremely broad possibility as there is always a written or oral contract with a health professional (even for instance for advertisement purposes).
The contract is not foreseen for instance under Article 9 of the GDPR (only under 9.2 h but with a link with a legitimate medical purpose). I would add a reference to the contract **for health related purposes** (to avoid for instance the processing for advertisement purposes, etc)

Comment [A58]: What would be the examples of further processing of genetic data collected in the context of a judicial procedure/investigation? We could just delete this reference to domestic law if there is no legitimate need in practice.

7.4 Any processing of genetic data prescribed by law other than in the cases provided for in paragraphs 7.2 and 7.3 should only be carried out to avoid any serious prejudice to the health of the data subject or of a member of her or his biological family or for reasons in relation with humanitarian action.

7.5 Existing predictive data resulting from genetic tests should not be processed for insurance purposes, except where this is specifically provided for by law. In that case, their processing should only be authorised in full respect of the applicable criteria defined by law, in light of the type of test used and the particular risk concerned. The provisions of Recommendation (2016)8 on the processing of personal health-related data for insurance purposes, including data resulting from genetic tests are also to be taken into consideration in that regard.

7.6 The data subject is entitled to know any information collected about her or his health. However, the wish of the person whose genetic data are analysed not to know should be taken into consideration, and that person should be informed, prior to such analysis, of the possibility of not being informed of the results, including of unexpected findings. Her or his wish not to know may, in her or his interests or in the interests of a member of her or his biologic family, have to be restricted as foreseen by law, notably in light of the doctors' duty to provide care.

~~7.7 The publication of genetic data which would identify the data subject or a person who has a direct link with her or his genetic line, should be prohibited, except where the data subject has expressly consented beforehand to it and it is prescribed by law, for specific purposes and with the appropriate safeguards.~~

8. Shar~~ed professional secrecy~~ing of health-related data for purposes of providing and administering health care

8.1 Where health-related data are shared by different professionals for purposes of providing and administering health care of an individual, the data subject ~~should~~ shall be informed beforehand, except where this proves to be impossible due to an emergency, of the nature of the health-related data processed and of the health professionals participating in the provision of care. The data subject must be able, in accordance with safeguards prescribed by law, to withdraw consent, where such consent is required by law, or object at any time to the exchange and sharing of her or his health-related data.

8.2 ~~In the interests of greater co-ordination between p~~Professionals operating on a particular individual case in the health and medico-social sector and sharing data in the interests of greater co-ordination should be subject to professional confidentiality incumbent upon a health-care professional, or to equal rules of confidentiality~~, the domestic law 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 should be limited to the information strictly necessary for the co-ordination or continuity of care, prevention or medico-social and social follow-up of the individual, with the respective actors only able in this case to share or receive data lying strictly within the scope of their tasks and depending on their authorisations. Appropriate measures should be taken to ensure the security of the data.

8.4 The use of an electronic medical file and of an electronic mailbox allowing for the sharing and exchange of health-related data should respect those principles.

9. Communication ~~to 'authorised recipients'~~of health-related data

9.1 Health-related data may be communicated to recipients where the latter are authorised by ~~domestic~~ law to have access to the data. ~~Such authorised recipients may be judicial authorities, experts appointed by a court authority, members of staff of an administrative authority designated by a legal formal act or humanitarian organisations, among other people.~~

9.2 ~~Medical officers of i~~Insurance companies and employers cannot, in principle, be regarded as recipients authorised to have access to the health-related data of patients unless domestic law makes provision for this with appropriate safeguards and if the data subject has validly consented to it.

Comment [A59]: I am not sure I understand this reference to the nature of the health professionals that would justify the lack of information to individuals. Perhaps the expert will be able to give one example? Moreover, I am not sure that the wording of this section is fully consistent with section 11.2

Comment [A60]: Is there an overlap between the titles of sections 8 and 9? These sections could be merged. Alternatively, section 9 could concern the sharing of health data for other purposes (than health related purposes)

Comment [A61]: This paragraph is a bit too broad. What kind of health related data? Who are the recipients?

9.3 Health-related data will, unless other appropriate safeguards are provided for by ~~domestic~~ law, only be communicated to an authorised recipient who is subject to the rules of confidentiality incumbent upon a health-care professional, or to equal rules of confidentiality.

Comment [A62]: This sentence a bit strange like that, perhaps use "can" instead of "will"?

10. Storage of health-related data

The data should not be stored in a form which permits identification of the data subjects for longer than is necessary for the purposes for which they are processed unless they are used for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes and where appropriate measures enable to safeguard the rights and fundamental freedoms of the data subject. In this case, data should in principle be anonymised as soon as the research, the archiving activity or the statistical study enables it.

1.21 Chapter III. The rights of the data subject

11. Transparency of processing

11.1 The data subject must be informed by the controller of the processing of their health-related data before the data are processed.

The information must include:

- 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,
- the length of ~~conservation~~ preservation of the data,
- the recipients or categories of recipients of the data, and planned data transfers to a third country, or an international organisation,
- the possibility, if applicable, of objecting to the processing of their data, in the conditions prescribed in paragraph 12.2,
- the conditions and the means made available to them for exercising via the controller their rights of access, the right of rectification and the right to erasure of their health-related data.

The information must where necessary, with a view to ensuring a fair and transparent processing, also include:

- that their data may subsequently be processed for a compatible purpose, in accordance with appropriate safeguards provided for by domestic law and in the conditions prescribed in paragraph 4.1.b,
- the specific techniques used to process their health-related data,
- the possibility of lodging a complaint with a supervisory authority or in front of the court,
- the existence of automated decisions, including profiling ~~where~~ which is only permissible where prescribed by~~domestic~~ law ~~allows~~ and~~it~~ subject to appropriate safeguards.

11.2 This information should be provided prior to data collection or at the first communication, unless it proves impossible or requires disproportionate efforts from the controller, in particular for processing for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes.

11.3 The information must be intelligible and easily accessible, in a clear and plain language and suited to the circumstances to allow a full understanding of the processing by the data subject. In particular, where the data subject is physically or legally incapable of receiving the information, it may be given to the person legally representing her or him. If a legally incapacitated person is capable of understanding, he or she should be informed before the data are processed.

11.4 Only urgency or the impossibility for the data subject to be informed can give rise to an exemption from the obligation of informing. In such a case, information should be provided as soon as possible.

11.5 A person's wish to be kept in ignorance of a diagnosis or prognosis should be complied with, except where this constitutes a serious risk for the health of third parties.

11.6 Domestic law should provide for appropriate safeguards ensuring respect for these rights.

12. The rights of access, objection, rectification, erasure and data portability

12.1 The data subject has the right to know whether personal data which concern her or him are being processed, and, if so, to obtain - without excessive delay or expense and in an intelligible form - communication of her or his data and to have access~~, without excessive delay or expense and in an intelligible form,~~ in the same conditions to at least the following information:

- the purpose or purposes of the processing,
- the categories of personal data concerned,
- the recipients or categories of the recipients of the data and the envisaged data transfers to a third country, or an international organisation,
- the preservation period,
- the knowledge of the reasoning underlying data processing where the results of such processing are applied to her or him, notably in the case of profiling.

12.2 The data subject has the right to erasure of data processed against the principles of this Recommendation~~is exercised subject to legitimate grounds~~. The data subject is entitled to obtain rectification of data concerning her or him. The data subject furthermore has the right to object on grounds relating to her or his personal situation to the processing of her or his health-related data, unless it is anonymised or the controller demonstrates an overriding and legitimate reason for pursuing the data processing.

12.3 If the request to rectify or erase the data is refused or if the data subject's objection is rejected, he or she should be able to ~~appeal~~have a remedy.

12.4 The right to data portability ~~enables the data subject to~~ requires, subject to conditions prescribed by law, from the controller, where the processing is performed by automatic means, the transmission - in a structured, interoperable and machine-readable format - of her or his personal data with a view to transmitting them to another controller. The data subject can also require from the controller that he or she transmits directly the data to another controller.

12.5 The rights of data subjects should be easy to exercise and all States ~~must~~ should ensure that every person is given the necessary and ~~,~~ adequate, ~~legal, effective and practical~~ means to exercise their rights.

12.6 Health professionals have to put in place all necessary measures in order to ensure respect for the effective exercise of such rights as an element of their professional deontology, as recognised by domestic law.

12.7 The rights of data subjects can be subject to restrictions provided for by law, where such restrictions are necessary and proportionate measures in a democratic society for the reasons specified in Article 9 of Convention No.108, notably objectives of general public interest of the State relating to public health.

1.22 Chapter IV. ~~Reference frameworks of i~~ Security and interoperability

~~**13. Reference frameworks**~~

~~13.1 Interoperability of systems enables to contribute to data portability and should for this reason be encouraged. The processing of health-related data furthermore requires that all players observe high standards to ensure the lawfulness of the processing and security and confidentiality of such data. Reference frameworks, offering a technical frame, may facilitate interoperability and security.~~

~~13.2 Reference frameworks should be taken into consideration at the design stage of information systems and compliance with them is of particular importance where health-related data are collected~~

~~and processed in connection with care and treatment.~~
~~Reference frameworks defined by the stakeholders and based on international norms aim at setting standards enabling the portability, exchange and sharing of health-related data by information systems and at facilitating the monitoring of their implementation under the conditions of security required, for instance through certification schemes.~~

13~~5~~. Security ~~reference frameworks~~

1~~5~~3.1 The processing of health-related data is to be made secure and security ~~policies~~ measures adapted to the risks for fundamental rights and freedoms must in that regard be defined to ensure that all players observe high standards guaranteeing the lawfulness of the processing and security and confidentiality of such data.

1~~5~~3.2 These security rules, defined by domestic law and possibly contained in reference frameworks, constantly kept state-of-the-art and regularly reviewed, should result in the adoption of ~~such~~ technical and organisational measures as to protect personal health-related data from any illegal or accidental destruction, any loss or any impairment, and to guard against any unauthorised access or unavailability or inaccessibility. In particular, ~~domestic~~ the law should make provision for organising and regulating procedures concerning the collection, storage and restitution of health-related data.

13~~5~~.3 System availability – i.e. the proper functioning of the system – 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.

13~~5~~.4 Guaranteeing integrity requires verification of every action carried out on the data, any changes made to or deletion of data, including the communication of data. It also requires the establishment of measures to monitor access to the data base and the data themselves, ensuring that only authorised persons are able to access the data.

13~~5~~.5 Auditability should lead to a system making it possible to trace any access to the information system and modifications made and for any action carried out, to be able to identify its author.

13~~5~~.6 Activity entailing hosting health-related data and making them available for users should comply with the security reference framework and principles of personal data protection.

13~~5~~.7 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-related data. They must have full regard for professional secrecy and comply with appropriate measures laid down in ~~domestic~~ law to guarantee the confidentiality and security of the data.

14. Interoperability ~~reference frameworks~~

~~**13. Reference frameworks**~~

14~~3~~.1 Interoperability of systems enables to contribute to data portability and should for this reason be encouraged. ~~The processing of health-related data furthermore requires that all players observe high standards to ensure the lawfulness of the processing and security and confidentiality of such data.~~ Reference frameworks, offering~~ing~~ a technical frame, ~~may~~ facilitating~~e~~ interoperability based on international norms should ensure that a high level of security is guaranteed while providing for such interoperability. The monitoring of the implementation of reference frameworks can be done through certification schemes ~~and security~~.

14.2 Reference frameworks should be taken into consideration at the design stage of information systems.

Comment [A63]: stakeholders? involved actors?

Comment [A64]: This section does not really describe what is interoperability and the need to take into account data protection safeguards. It starts with a link with data portability which is not in my view the initial aim of interoperability. This section could be furthered detailed.

One might find some ideas (that obviously need to be adapted for such a recommendation) in the EDPS recent reflection paper on the topic (cf. https://edps.europa.eu/sites/edp/files/publication/17-11-16_opinion_interoperability_en.pdf),:
- Interoperability is commonly referred to as the ability of different information systems to communicate, exchange data and use the information that has been exchanged
- interoperability may help address some needs of competent authorities using large scale information systems as well as reduce the overall cost of operating such systems.
- Interoperability may even provide some benefits in terms of data protection (up-to-date information, avoid that identical data are stored in multiple databases):
- however, interoperability should not be an end in and of itself, but should always serve a genuine public interest objective ;
- as interoperability is likely to imply new (or changed) personal data processing, such changes would require a clear basis in legislation;
- any new or modified data processing would need to be clearly defined and be equally necessary and proportionate in relation to its clearly stated objectives;
- the specific purposes of the envisaged data processing should be clearly defined;
- strong data protection safeguards should be put in place when using interoperable systems (in terms of access, defining new uses, new security measures, etc)

1.23 Chapter V. Scientific research

15~~6~~. Scientific research

1~~6~~5.1 The processing of health-related data for the purposes of scientific research should be subject to appropriate safeguards, complementing the other provisions of the present recommendation, and be carried out with a legitimate aim for the rights and fundamental freedoms of the data subject.

1~~6~~5.2 The need to process health-related data for the purposes of scientific research should be evaluated in the light of the aim pursued and the risks to the data subject and, in relation to genetic data to her or his biological family.

1~~6~~5.3 The data subject should, in addition to what is foreseen in Chapter III be provided with prior, transparent and comprehensible information that is as precise as possible with regard to:

- the nature of the envisaged scientific research, the possible choices that he or she could exercise as well as any relevant conditions governing the use of the data, including re-contact and feedback;
- the conditions applicable to the storage of the data, including access and possible communication policies; and
- the rights and safeguards provided for by law, and specifically of her or his right to refuse to participate in the research and withdraw at any time.

Restrictions may be applied in the event of a medical emergency provided that appropriate safeguards are ensured.

1~~6~~5.4 As it is not always possible to determine beforehand the purposes of different research projects at the time of the collection of data, data subjects should be able ~~–~~to exercise a choice solely for certain ~~fields~~ areas of research or certain parts of research projects, to the extent allowed by the intended purpose, with due regard for recognised ethical standards.

15~~6~~.5 Health-related data should only be used in a research project if the data subject, after having received prior information according to the provisions of paragraph 15~~6~~.3, has consented to it or, if permitted by law providing appropriate safeguards, has not objected to it. If the proposed use of the data in a research project is not explained prior to collection of the data, reasonable efforts should be made to contact the data subject. The wish of the data subject not to be contacted should be observed. Where the attempt to contact the data subject proves unsuccessful, the health-related data should only be used in the research project subject to an independent evaluation of the fulfillment of the following conditions:

m. evidence is provided that reasonable efforts have been made to contact the person concerned;

n. the research addresses an overriding scientific interest and the processing is proportionate to the objective pursued ;

o. the aims of the research could not reasonably be achieved without using the data for which consent cannot be obtained; and

p. there is no evidence that the person concerned has expressly opposed such research use.

1~~6~~5.6 The conditions in which health-related data are processed for scientific research must be assessed, where necessary, by the body or bodies designated by ~~domestic~~ law.

Comment [A65]: Shouldn't it be "independent body or bodies designated by law" in order to be consistent with the requirement for an "independent evaluation" in 15.5?

1~~6~~5.7 Healthcare professionals who are entitled to carry out their own medical research and scientists in other disciplines should be able to use the health-related data which they hold as long as the data subject has been informed of this possibility beforehand in compliance with paragraph 15~~6~~.3 and subject to complementary safeguards determined by ~~domestic~~ law such as requiring explicit consent or the assessment of the competent body designated by law.

165.8 Where possible, data should be anonymised and where it is not possible, pseudonymisation of the data, with intervention of a trusted third-party at the separation stage of the identification, is among the measures that should be implemented to safeguard the rights and fundamental freedoms of the data subject. This must be done where the purposes of the scientific research can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects.

165.9 Where a data subject withdraws from a scientific research, her or his health-related data processed in the context of that research should be destroyed or anonymised in a manner not to compromise the scientific validity of the research and the data subject should be informed accordingly.

156.10 Personal data used for scientific research should not be published in a form which enables the data subjects to be identified, except where he or she has consented to it and domestic law allows it.

1.24 Chapter VI – Mobile applications

~~Mobile applications enable the development of new practices in the medical and public health fields. They include applications used in our daily lives of « quantified self » connecting to medical devices as well as systems of personal advice and monitoring.~~

167. Mobile applications

176.1 Where the data collected by these applications, whether implanted on the person or not, may reveal information on the physical or mental state of a person in connexion with her or his health or concern any information regarding health care and medico-social provision, they constitute health-related data. In this connection they enjoy the same legal protection and confidentiality applicable to other health-related data processing as defined by the present Recommendation and, where applicable, supplemented by the domestic law.

176.2 Persons using such mobile applications, as soon as they involve the processing of their personal data, must enjoy the same rights as those provided for in Chapter III of the present Recommendation. They must notably have obtained beforehand all necessary information on the nature and functioning of the system in order to be able to control its use. To this effect clear and transparent information on the intended processing should be drafted by the controller with the participation of the software designer and the software distributor whose respective roles have to be determined in advance.

176.3 Any use of mobile applications must be accompanied by specific, tailored and state-of-the-art security measures which notably provide for the authentication of the person concerned and the encryption of the transmission of data.

167.4 The hosting, by a third party of health-related data produced by mobile applications must obey security rules providing for the confidentiality, integrity and restitution of the data upon request of the data subject.