COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 23 June / juin 2017

T-PD(2017)04MosAdd

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

AUSTRIA / AUTRICHE

Concerning the Draft Recommendation on the protection of health-related data the Austrian Data Protection Authority proposes the following amendments:

Chapter III, Principle 11:

In para. 11.4. the sentence should read: „The right to portability enables the data subject to require where applicable and as far as possible from the controller the transmission […]."

The current wording goes beyond Art. 20 (1) GDPR and would impose heavy burdens on ordinary health professionals without technical support.

CYPRUS / CHYPRE

Draft recommendation on the protection of health-related data

Cyprus Comments

Principle 6 – Data concerning unborn children
This principle determines that health-related data concerning unborn children (…) should enjoy a protection comparable to the protection provided to **health-related data of a minor**. However, this draft recommendation does not provide for any principles regulating the protection of health related data of minors.

We are not sure the manner in which principle 6 could be implemented in practice by State Parties, unless national law foresees special provisions on the protection of health-related data of minors. Perhaps this could be clarified in the explanatory memorandum or alternatively the words "*as provided for in national law*'' could be added after the end of the sentence. In such a case principle 6 will read as follows:

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 a foetus should enjoy a protection comparable to the protection provided to health-related data of a minor, ***as provided for in national law****.*

Principle 8 - Shared medical secrecy for purposes of providing and administering care
Paragraph 8.1 – Unless there is a specific purpose to recall the obligation of the controller to inform the data subject in principle 8, for the sake of clarity it might be more appropriate to transfer the provisions of this paragraph (first sentence) in principle 12.1 which deals with the transparency of the processing.

Principle 11 - The rights of access, objection, rectification, erasure and portability
Paragraph 11.1 - It is not clear whether this paragraph deals with the right of access or the right to be informed or both. If it deals solely with the right of access then we propose the following modification in the first half:

"Everyone has the right to have access to personal data being processed, which concern him or her and to obtain, on request, without excessive delay or expense and in an intelligible form, the following information:…"

We further suggest adding in the second part of paragraph 11.1 that the data subject may request a **copy** of the information comprising the data and to be given details of the **source** of the data, where applicable.

Paragraph 11.3 –the explanatory memorandum should clarify which are the likely competent authorities to receive such an appeal.

Paragraph 11.5 – the use of the word ''States'' in this paragraph is unclear. Perhaps a more appropriate word would be ''data controller''?

Principle 12 – Transparency of processing
For the sake of clarity we suggest transferring principle 12 before principle 11.

Paragraph 12.4 – words ''these rights'' should be singular ''this right''

Principle 16 – Security reference frameworks
Paragraph 16.2 – we suggest amending as follows in order to connect with the following paragraphs:

Domestic law should make provision for organising and regulating health-related data collection, storage and restitution procedures ***and notably to guarantee system's availability, integrity and auditability****.*

Paragraph 16.4 – In our view the second part of the paragraph starting ''It also requires the establishment..'' would be more appropriate under paragraph 16.5?

Principle 17 – scientific research
Paragraph 17.2 – this principle is unclear (it is perhaps due to the translation from French). We suggest the following rewording:

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

Paragraph 17.3 – in the first part, consider replacing the word ''comprehensible'' by ''intelligible''.

In the list of information that should be provided to the data subject we refer to the ''possible choices that he or she could exercise''. Do we refer here to the choices foreseen in paragraph 17.4? It is perhaps useful to mention it in brackets.

Paragraph 17.6 – It is essential to guarantee the supervision of <u>all</u> scientific researches by a public body or bodies (e.g. bioethics committee) in order to safeguard the right to data protection as well as the protection of other human rights, when health-related data are used for the purposes of scientific research. We suggest deleting ''where necessary''.

DENMARK / DANEMARK

Comments from Denmark - draft recommendation on the protection of health-related data

General remarks
In our opinion the draft recommendation still needs a thorough revision before it can be considered for adoption. Our main concerns are:

- The draft recommendation needs to be brought in line with the rules in the General Data Protection Regulation (EU)
- Several points needs thorough revision – especially point 17 on scientific research and points concerning the rights of the data subjects

Detailed comments

1. Proposal concerning paragraph 11 and 12:

Article 12 should be merged with article 11, in order to make sure, that article 11.7, that states that, 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, also comprehend the right to be informed, which is implied in article 12.

Justification of the proposal:

According to article 11.7, the rights of data subjects must be reconciled with other legitimate rights and interests, and they 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.

Article 12, concerning "Transparency of processing" does not have a similar paragraph to article 11.7.

In order to make sure that the member states have the possibility to restrict the right to be informed in the same way as the member states can restrict other rights of the data subject, Denmark suggests, that the two articles are merged.

2. Proposal concerning paragraph 5 and 17

5. Purposes and legitimate basis of health-related data processing
5.1 …
f. for processing for archiving purposes in the public interest, for scientific or historical research purposes or statistical purposes under 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 legitimate interests;

17.3 The person concerned should generally be provided with prior, transparent and comprehensible information about the scientific research and its purpose unless it requires disproportionate efforts to inform each individual person. Information about the scientific research and purpose should in such cases, however, still be provided publically in order to ensure transparency regarding the use of health care data. Persons whose data are being used for research must, where provided for in

domestic law, give their consent, except in cases of medical emergency. The information provided to the person concerned should be ~~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 recontact and feedback;
– the conditions applicable to the storage of the data, including access and possible transfer 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.

~~17.9 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 and the ~~data subject should be informed accordingly unless it requires disproportionate efforts.~~A data subject can at any time withdraw from a scientific research. The withdrawal does not affect the access to processing the data subject's health-related data that already forms part of the scientific research.

Justification of the proposal
It is of great importance to Denmark to find the right balance between protecting the individual's right to protection of their health data and the possibility of register-based research in the health field.

Under Danish law a data subject can withdraw from a scientific research at any time. The revocation, however, does not affect the access to processing the data subject's personal information that has already been processed in the research project. It may require disproportionate efforts and be seriously detrimental to the research project to destroy or anonymise the data already processed in the scientific research.

Denmark consequently proposes a change of the wording of paragraphs 5.1. f, paragraph 17.3 and 17.9 on research in the health field.

GERMANY (DPA)

TABLE OF CONTENTS

Recommendation

CM/Rec(2017)…. of the Committee of Ministers to member States on the protection of health-related data

(adopted by the Committee of Ministers … 2017,
at the … meeting of the Ministers' Deputies)

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 computerisation of the health sector 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 potentially identifying, coupled to the technical analysis capacities linked to personalised health care be accompanied of legal and technical measures enabling an effective protection of every individual.

People's desire to have more control over their data and the decisions based on the processing of such data is another feature of this change. Noteworthy features of this new environment are the growing computerisation of the professional sector and particularly of activities relating to care and prevention, to life sciences research and to health system management, and also the increasing involvement of patients in understanding the manner in which decisions concerning them are being taken.

Besides, geographical mobility accompanied by the development of medical devices and connected objects is 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 the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 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 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(2017)…

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 interoperable and secured information systems in a manner enabling the quality of care and the efficiency of health systems to be enhanced.

2. Scope

This Recommendation is applicable to the processing of personal data relating to 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 which contribute to the respect for the rights of every individual and the confidentiality of data.

The provisions of this Recommendation do not apply to health-related data processing performed by individuals in the context of exclusively 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. An individual shall not be regarded as “identifiable” if identification requires unreasonable time, effort or other resources.. In cases where the individual is not identifiable, the data are considered as anonymous.

- 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 make a data item non-identifying as long as it is not associated with other elements which are kept separately in a secure and organised manner and which would make direct or indirect identification of a person possible. 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 “data 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 an individual or legal entity, public authority, service or other organisation which processes data for a data 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.

- 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 hosting service providers irrespective of the platform used for the secure and lasting digital storage of data.

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 (see principle 5) and must not be processed in a manner which is incompatible with these purposes. Subsequent processing by the same processor 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 (with respect to guarantees applicable to scientific research for instance, see principle 17) 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 13 or on other legitimate basis laid down by law as laid down in principle 5 of the present recommendation.

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 limited to what is necessary ~~not excessive~~ in relation to the purposes for which they are processed; they must be accurate and, if necessary, updated.

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 personal data or the destruction, loss, use, unavailability, inaccessibility, modification or disclosure to unauthorised persons of those 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 11 of the present recommendation.

4.2 Data controllers and their processors who are not health professionals should only process health-related data in accordance with similar rules of confidentiality and security measures that apply to health professionals.

Comment [BfDI 1]: Clarification proposed.

Comment [BfDI 2]: Proposal to align the wording with the definition of the principle of data minimisation in Art. 5 No. 1 (c) GDPR.

Formatted: Font: 10 pt

5. Purposes and legitimate basis of health-related data processing

5.1 Health-related data may be processed for the following purposes where such processing is foreseen by law and appropriate safeguards are provided:

a. 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;

b. for reasons of public interest in the public health sector, 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;

c. for the purpose of safeguarding the vital interests of the data subject or of another person;

d. for reasons of public interest in the field of managing claims for social welfare and health insurance benefits and services;

e. for reasons of public health compatible with the initial purpose of the collection of data, provided that they are lawful and;

f. for processing for archiving purposes in the public interest, for scientific or historical research purposes or statistical purposes under 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 legitimate interests;

g. for reasons relating to the obligations of the controllers and to the exercise of their rights or those of the data subject regarding employment and social protection, in accordance with domestic legislation or any collective agreement complying with the said legislation and providing for appropriate safeguards;

h. 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 in accordance with principle 13 of this recommendation, 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.

5.3 Health-related data may also be processed where the processing is based on a contract entered into with a health professional.

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.

5.5 Personal data protection principles must be taken into account 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. The controller should assess the impact of the applications used in terms of data protection and respect for privacy.

5.6. Controllers 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 for which they are responsible is in line with those obligations.

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 a foetus should enjoy a protection comparable to the protection provided to health-related data of a minor.

7. Genetic data

7.1 Genetic data should only be collected where it is provided for 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 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. In no case should such data be used to determine other characteristics which may be linked genetically.

7.4 Any processing of genetic data 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 after an independent assessment of the respect of the applicable criteria defined by law, in light of the type of test used and the particular risk concerned.

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 respected, 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. Shared medical secrecy for purposes of providing and administering care

8.1 The data subject should 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 to 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 professionals operating in the health and medico-social sector, the domestic law of each member State (is to) may recognise a shared professional secrecy, between professionals who are themselves legally bound by such secrecy.

Comment [BfDI 3]: Proposal to replace "is to" by "may"

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 monitoring of the individual, with the respective actors only able in this case to pass on or receive data lying strictly within the scope of their tasks and depending on their authorisations.

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 at least those principles.

9. Communication to 'authorised recipients'

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 an official text or humanitarian organisations, among other people.

9.2 Medical officers of 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 or if the data subject has, in accordance with domestic law, consented to it.

Comment [BfDI 4]: Clarification proposed.

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 similar rules of confidentiality.

10. Storage of health-related data

10.1 The data must not be stored in a form which permits identification of the data subjects for no 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. If the data are used for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes, the data should, in principle, be anonymized as soon as the research, archiving or statistical purposes allow this.

Comment [BfDI 5]: See for instance § 27 para 3 DSAnpUG-EU

10.2 Storage of health-related data for other purposes than those for which they were initially collected should be carried out in compliance with the principles of this Recommendation, notably with respect to the compatibility of the purposes of such further processing with the purposes of the initial processing.

Chapter III. The rights of the data subject

11. The rights of access, objection, rectification, erasure and portability

11.1 Everyone has the right to know whether personal data which concern them are being processed, and, if so, to have access, without excessive delay or expense and in an intelligible form, at least to the following information:

Comment [BfDI 6]: It should be possible, that the data subject receives more 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 length of conservation of the data,
- the knowledge of the reasoning underlying data processing where the results of such processing are applied to her or him.

11.2 The right to erasure is exercised subject to the cases prescribed by law and invoking 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, unless the person holding the data invokes an overriding and legitimate reason concerning the general interest of public health or unless data are being processed according to the conditions prescribed in principle 17.

11.3 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.

11.4 The right to portability enables the data subject to require from the controller the transmission of her or his personal data processed by automatic means to another controller, in a structured, interoperable and machine-readable format.

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

11.6 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.

11.7 The rights of data subjects must be reconciled with other legitimate rights and interests. They 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.

12. Transparency of processing

12.1 Everyone must be informed 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 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 11.2,
- 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 should 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.

Comment [BfDI 7]: : It should be added that according to Art. 22 No.4 GDPR automated decisions are, in principle, not taken on the basis of health data.

12.2 This information should be provided at the time of data collection or of the first communication, unless it proves impossible or requires disproportionate efforts from the controller, in particular for processing for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes. It must be appropriate and suited to the circumstances. In particular, where the data subject is physically or legally incapable of receiving the information, it may be given to the person legally representing her or him. If a legally incapacitated person is capable of understanding, he or she should be informed before the data are processed. Only urgency or the impossibility of providing information can give rise to an exemption from the obligation of transparency. In such a case, information should be provided as soon as possible.

12.3 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.

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

13. 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. When the consent is given by electronic means, proof of its expression should be made possible by any technical process.

Chapter IV. Reference frameworks of interoperability and security

14. Reference frameworks

14.1 Interoperability of systems enables to contribute to the portability of data and should for this reason be encouraged. The processing of health-related data furthermore requires that all players observe high standards to ensure the confidentiality of such data.
14.2 The development of efficient information systems, guaranteeing the respect of human rights of the data subject, aims at enhancing the health monitoring of a person during her or his treatment. To this end, health professionals as well as any public or private organisation authorised to process health-related data, in particular persons responsible for applications allowing exchange and sharing of health-related data, must comply with reference frameworks to which each domestic law of a country can attribute a legally binding effect.

15. Interoperability reference frameworks

15.1 The aim of these reference frameworks is to define standards enabling the portability, exchange and sharing of health-related data by information systems and to monitor their implementation under the conditions of security required, for instance through certification schemes.

15.2 Consideration of the reference frameworks has to be integrated by design (*privacy by design*) and compliance with them is of particular importance where health-related data are collected and processed in connection with care and treatment.

16. Security reference frameworks

16.1 The processing of health-related data is to be made secure and security policies adapted to the risks for fundamental rights and freedoms must in that regard be defined.

16.2 These security rules, kept constantly 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 law should make provision for organising and regulating health-related data collection, storage and restitution procedures.

16.3 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.

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

16.5 Auditability should lead to a system making it possible to trace any access to the information system and for any action carried out by an individual to be logged to that individual.

16.6 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.

16.7 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 with appropriate measures laid down in domestic law to guarantee the confidentiality and security of the data.

Chapter V. Scientific research

17. Scientific research

17.1 The processing of health-related data for the purposes of scientific research must, in addition to the other prescriptions of this text, be carried out with a legitimate aim and in full compliance with the principles of protection of human rights applied to this particular field.

17.2 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.

17.3 The person concerned should, in addition to the provisions of 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 transfer 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.

(~~17.4~~ 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 of research or certain parts of research projects, to the extent allowed by the intended purpose.)

17.5 Health-related data should only be used in a research project if the latter is within the scope of the acceptance given by the data subject. If the proposed use of the data in a research project is not within this scope, acceptance of the proposed use should be sought and, to this end, 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 important 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.

17.6 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.

17.7 Healthcare professionals who are entitled to carry out their own medical research and scientists in other disciplines should, on the basis of the relevant legal grounds, 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 17.3.

17.8 Pseudonymisation of the data, with intervention of a trusted third-party at the separation stage of the identification, is among the measures that can be implemented to safeguard the rights and fundamental freedoms of the data subject. This should be preferred 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 [BfDI 8]: Clarification proposed.

Comment [BfDI 9]: Clarification proposed.

Comment [BfDI 10]: In light of the GDPR and the strict conditions stated by Art. 9 para 2 a) in relation to the consent regarding the processing of special categories of data like health data this paragraph should be deleted.

Comment [BfDI 11]: Clarification proposed.

Comment [BfDI 12]: Should pseudonymisation generally be preferred to anonymization?

17.9 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 and the data subject should be informed accordingly.

17.10 Personal data used for scientific research may not be published in a form which enables the data subjects to be identified.

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

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.

18. Mobile applications

18.1 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 social provision and/or are processed in a medical context, they constitute health-related data. In this connection they should 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 of States.

Comment [BfDI 13]: Proposal to align the definition with Chapter 1 No. 3/GDPR.

18.2 Persons using such mobile applications, as soon as they involve the processing of their personal data, must enjoy similar rights to 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 terms and conditions 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.

18.3 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.

18.4 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.

GERMANY (GOVERNMENT)

Strasbourg, 1 June 2017

T-PD(2017)03

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

DRAFT RECOMMENDATION ON THE PROTECTION OF HEALTH-RELATED DATA

Comment [A14]: General remarks: In our view the draft still needs profound revision and is not yet ready for adoption. Here are some key points:

1. The draft still has to be brought in line with the GDPR. This is inter alia relevant when it comes to the rights of the data subjects and the area of scientific research.

2. The part on genetic data (7.) still needs thorough revision. Particularly, the level of protection reached by the Additional Protocol of 2005 to the Convention on Human Rights and Biomedicine ("Oviedo Convention") concerning Biomedical Research should not be lowered by the present draft. In this context it should also be clarified that Section 7 only deals with **health-related** genetic data. The text in its current version appears contradictory and therefore unclear.

3. The part on scientific research (17.) still needs to be intensively worked on.

4. We do have a scrutiny reservation on the entire Chapter IV ("reference frameworks") because the content of this chapter remains unclear.

Please find detailed comments on the different parts of the text below.

Directorate General Human Rights and Rule of Law

TABLE OF CONTENTS

Recommendation

CM/Rec(2017)…. of the Committee of Ministers to member States on the protection of health-related data

(adopted by the Committee of Ministers … 2017,
at the … meeting of the Ministers' Deputies)

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 computerisation of the health sector 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 potentially identifying, coupled to the technical analysis capacities linked to personalised health care be accompanied of legal and technical measures enabling an effective protection of every individual.

People's desire to have more control over their data and the decisions based on the processing of such data is another feature of this change. Noteworthy features of this new environment are the growing computerisation of the professional sector and particularly of activities relating to care and prevention, to life sciences research and to health system management, and also the increasing involvement of patients in understanding the manner in which decisions concerning them are being taken.

Besides, geographical mobility accompanied by the development of medical devices and connected objects is 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 the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 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 [A15]: There is a substantial difference between medical data (i.e. data processed for medical purposes by health care professionals) and health data (data concerning the past, current or future state of health irrespective of the profession), or "data concerning health" in accordance with Article 4 (15) of the GDPR. Whatever term is used, it must be ensured that the broader scope of the recommendation does not dilute the specific data protection regime applied to health care professionals.

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;~~take into account the principles set forth in the appendix to the present Recommendation, which replaces Recommendation (97) 5 mentioned above

- 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.

Comment [A16]: This wording is supported. It is realistic now to ensure consistency with this Recommendation.

Appendix to Recommendation CM/Rec(2017)…

Chapter I. General provisions

19. 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 interoperable and secured information systems in a manner enabling the quality of care and the efficiency of health systems to be enhanced.

20. 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 which contribute to the respect for the rights of every individual and the confidentiality of data.

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

21. Definitions

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

- The expression "personal data" ~~refers to~~ means 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 other resources.~~.~~ In cases where the individual is not identifiable, the data are considered as anonymous.

- The expression "anonymisation" ~~refers~~ means ~~to~~ the processing of ~~applied to~~ personal data in such a manner ~~so~~ that the data subject~~s~~ is not ~~can~~ or no longer ~~be identified either directly or indirectly~~identifiable.

- The expression "pseudonymisation" ~~refers to a type of processing which makes it possible to make a data item non identifying as long as it is not associated with other elements which are kept separately in a secure and organised manner and which would make direct or indirect identification of a person possible.~~ 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.

Comment [A17]: The wording used above is "for the rights and fundamental freedoms of the individual". Would it not be better to use the same language wherever possible?

Comment [A18]: Alignment with Article 2 a) of Convention 108.

Comment [A19]: This part of the definition uses different wording than both the GDPR and Article 2 of the Convention 108. Also, it does not seem necessary to refer to the concept of anonymisation at this bullet point - anonymisation is covered by the next bullet point.

Comment [A20]: Suggested alignment with Recital 26 of the GDPR.

Comment [A21]: Please align to Article 4 (5) of the GDPR: "'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person".

Comment [A22]: It is suggested to use the exact wording of the definition in Article 4 (15) of the GDPR ("data concerning health"): "'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status".

Comment [A23]: Even though this is the language used in the Additional Protocol to the Convention on Human Rights and Biomedicine concerning Genetic Testing for Health Purposes, here it seems advisable to delete this word in order to avoid a lack of clarity with regard to which stage of prenatal development is meant. When exactly does "early" end?

Comment [A24]: Please align with Article 4 (13) of the GDPR. Differences from the definition in the GDPR should be avoided so as not to create the impression that the term means something different here.

- 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 “data 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 an individual or legal entity, public authority, service or other organisation which processes data for a data 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.

- 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 hosting service providers irrespective of the platform used for the secure and lasting digital storage of data.

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

22. 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 (see principle 5) and must not be processed in a manner which is incompatible with these purposes. Subsequent 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 (with respect to guarantees applicable to scientific research for instance, see principle 17) 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 13 or on other legitimate basis laid down by law as laid down in principle 5 of the present recommendation. Domestic law may foresee further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

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, updated.

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 personal data or the destruction, loss, use, unavailability, inaccessibility, modification or disclosure to unauthorised persons of those data.

Comment [A25]: Please align with Article 2 f) of the revised Convention 108 or with Article 4 (8) of the GDPR.

Comment [A26]: The definition is incomplete: It remains unclear who is responsible for coordinating, drafting and updating such a “reference framework”. It also remains unclear what legal quality the reference framework rules would have. Please explain if this definition is new or if there are existing examples.

Comment [A27]: The need for this definition which is not found in the GDPR or the Convention is unclear.

Comment [A28]: Better wording (no repetition!) appears to be necessary.

Comment [A29]: If the words “of the present recommendation” are added here, it would also be necessary to add them in all other places where reference is made to principles of the recommendation, in order to avoid that, where these words are not added, it is inferred that something else is meant.

Comment [A30]: Alignment with Article 9 (4) GDPR: Parties must remain free to impose even stricter rules when it comes to the processing of these very sensitive data. For example: Domestic law could forbid the processing of genetic data by a general physician - even if the data subject has given its consent. The domestic law could allow the processing of genetic data only if it the controller is a certified specialist in genetics.

This is also in line with Article 11 of the revised Convention 108 [“Extended protection”].

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 11 of the present recommendation.

4.2 Data controllers and their processors who are not health professionals should only process health-related data in accordance with ~~similar~~ legal requirements that ensure the same level of data protection as the rules of confidentiality and security measures that apply to health professionals.

23. Purposes and legitimate basis of health-related data processing

5.1 Health-related data may be processed for the following purposes where such processing is foreseen by law and appropriate safeguards are provided:

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;

j. for reasons of public interest in the public health sector, 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;

k. for the purpose of safeguarding the vital interests of the data subject or of another natural person;

l. for reasons of public interest in the field of managing claims for social welfare and health insurance benefits and services;

m. for reasons of public health compatible with the initial purpose of the collection of data, provided that they are lawful and;

n. for processing for archiving purposes in the public interest, for scientific or historical research purposes or statistical purposes under 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 legitimate interests;

o. for reasons relating to the obligations of the controllers and to the exercise of their rights or those of the data subject regarding employment and social protection, in accordance with domestic legislation or any collective agreement complying with the said legislation and providing for appropriate safeguards;

p. 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 in accordance with principle 13 of this recommendation, 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.

5.3 Health-related data may also be processed where the processing is based on a contract entered into with a health professional.

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.

5.5 Personal data protection principles must be taken into account 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. The controller should assess the impact of the applications used in terms of data protection and respect for privacy.

Comment [A31]: Why only similar rules? This has to be clarified. Why should the level of protection differ between health professionals and data controllers / processors?

Comment [A32]: Why do some of the following letters refer to domestic law (e.g. f, g)? The provisions of national law apply anyway.

Comment [A33]: Please chose a wording closer to Article 9 (2) h) of the GDPR. Moreover, when it comes to the processing for these purposes, the GDPR contains a further condition in Article 9 (3): The person processing the data must be subject to an obligation of secrecy.

Comment [A34]: Please chose a wording closer to Article 9 § 2 i) of the GDPR.

Comment [A35]: Please align with Article 9 § 2 c) of the GDPR which contains an additional requirement: The data subject must be physically or legally incapable of giving consent.

Comment [A36]: Please align with Article 9 § 2 b) of the GDPR.

Comment [A37]: Why is a separate clause needed? Please merge with b). Both refer to public health purposes. Please specify which public health reasons not covered by a public interest are meant?

Comment [A38]: See comment on 5.1 above.

Comment [A39]: Which cases are meant in particular as distinct from the cases mentioned in 5.2? It also needs to be specified who the contracting partner of the health professional is supposed to be: The data subject? A third party? Moreover, the sense of Article 7 § 4 of the GDPR needs to be reflected: "When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract."

5.6. Controllers 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 for which they are responsible is in line with those obligations.

24. 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 a foetus should enjoy a protection comparable to the protection provided to health-related data of a minor.

25. Genetic data

7.1 Genetic data should only be collected where it is provided for by law, and subject to appropriate safeguards.

7.2 Genetic data processed with a ~~preventive~~ predictive 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 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. In no case should such data be used to determine other characteristics which may be linked genetically.

7.4 Any processing of genetic data 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 after an independent assessment of the respect of the applicable criteria defined by law, in light of the type of test used and the particular risk concerned.

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 respected, 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 subjects concerned haves ~~ves~~ expressly consented beforehand to it and it is prescribed by law, for specific purposes and with the appropriate safeguards.

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

8.1 The data subject should 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 to 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 professionals operating in the health and medico-social sector, the domestic law of each member State ~~is may to~~ 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 monitoring of the individual, with the respective actors only able in this case to pass on or receive data lying strictly within the scope of their tasks and depending on their authorisations.

Comment [A40]: First of all, it is true that the human dignity of the embryo and the foetus must be protected. However, it seems that there is no European consensus that unborn children should be treated in a way comparable to minors in data protection law. To our understanding data protection law is applicable from the moment a person is born and, in general, ends with the death of this person. This is because the purpose of data protection law is to protect the right of personality of a (living) natural person. It appears, however, that the embryo and the foetus can legally be considered as a part of the mother. Therefore, the embryo and foetus would be protected by the data protection rights applicable to the mother.

Comment [A41]: Please align the wording: which law is referred to? Above, reference was frequently made to domestic law. Is something else referred to here?

Comment [A42]: This is the simple application of the principle of purpose limitation. Or should further processing be excluded? What if the data subject consents to further processing?

Comment [A43]: It is not exactly clear what the meaning or the purpose of this clause is.

Comment [A44]: The meaning of this sentence is unclear: Which forms of processing are to be prevented?

Comment [A45]: This

Comment [A46]: Please align the wording: Which law is referred to? Above, reference was frequently made to domestic law. Is something else referred to here?

Comment [A47]: The additional requirement ("only [...] authorised after an independent assessment") is not acceptable. Where the data processing operation takes place on the basis of a law, it is the responsibility of the data protection supervisory authorities and the courts to check whether the ...

Comment [A48]: Genetic data and the results gained from their analysis do not only regard the persons tested, but also persons biologically related to them. Therefore the publication of su ...

Comment [A49]: There needs to be a legal basis for the transfer of personal data between health professionals. If the data subjected consented to the transfers, the consent can be withdra ...

Comment [A50]: Terminology: The document is a recommendation, not a binding legal provision!

Comment [A51]: What does that mean? It terms of data protection law there always needs to be a legal basis for the transfer of personal data - even between two professionals who both ...

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 at least those principles.

27. Communication to 'authorised recipients'

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 an official text or humanitarian organisations, among other people.

9.2 Medical officers of 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 or if the data subject has 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 similar rules of confidentiality.

28. Storage of health-related data

10.1 The data ~~must~~ should not be stored in a form which permits identification of the data subjects for no 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. If the data are used for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes, the data should, in principle, be anonymized as soon as the research, archiving or statistical purposes allow this.

Comment [A52]: Terminology: The document is a recommendation, not a binding legal provision!

10.2 Storage of health-related data for other purposes than those for which they were initially collected should be carried out in compliance with the principles of this Recommendation, notably with respect to the compatibility of the purposes of such further processing with the purposes of the initial processing.

Comment [A53]: The sentence needs to be redrafted or deleted. Further processing can be allowed under certain conditions if the initial and the new purpose are compatible. If both purposes are incompatible there needs to be a new legal basis for the further processing.

In any event, 10.2 deals only with storage of data - which is less problematic than the actual further processing. Therefore, it is suggested to cover the problem of further processing and compatibility of purposes at a different place in this Recommendation.

Chapter III. The rights of the data subject

29. The rights of access, objection, rectification, erasure and portability

11.1 Everyone has the right to know whether personal data which concern them are being processed, and, if so, to have access, without excessive delay or expense and in an intelligible form, to 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 length of conservation of the data,
- the knowledge of the reasoning underlying data processing where the results of such processing are applied to her or him.

Comment [A54]: This part needs to be fully in line with the GDPR.

Comment [A55]: What cases are meant?

11.2 The right to erasure is exercised subject to the cases prescribed by law and invoking 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, unless the person holding the data invokes an overriding and legitimate reason concerning the general interest of public health or unless data are being processed according to the conditions prescribed in principle 17.

Comment [A56]: An exception for medical documentation is necessary.

11.3 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.

11.4 The right to portability enables the data subject to require from the controller the transmission of her or his personal data processed by automatic means to another controller, in a structured, interoperable and machine-readable format.

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

11.6 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.

11.7 The rights of data subjects must be reconciled with other legitimate rights and interests. They 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.

30. Transparency of processing

12.1 ~~Everyone~~ The data subject ~~must~~ should be informed by the controller of the processing of ~~their~~ her or his health-related data.

The information ~~must~~ should 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 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, under~~in~~ the conditions prescribed in paragraph 11.2,
- 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 ~~should~~ may include:

- a hint that their data may subsequently be processed for a compatible purpose, in accordance with appropriate safeguards provided for by domestic law and under~~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.

12.2 This information should be provided at the time of data collection or of the first communication, unless it proves impossible or requires disproportionate efforts from the controller, in particular for processing for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes. It must be appropriate and suited to the circumstances. In particular, where the data subject is physically or legally incapable of receiving the information, it may be given to the person legally representing her or him. If a legally incapacitated person is capable of understanding, he or she should be informed before the data are processed. Only urgency or the impossibility of providing information can give rise to an exemption from the obligation ~~of transparency~~to inform the data subject. In such a case, information should be provided as soon as possible.

~~12.3 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.~~

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

Comment [A57]: Please align with Article 20 GDPR. E.g. this right exists only if it is technically feasible.

Comment [A58]: What exactly does this mean? Are implementations in the Rules of Professional Practice necessary? Is should be kept in mind that domestic law already contains binding legal obligations and sanctions.

Comment [A59]: Article 9 should be quoted in a precise manner in order to avoid inaccuracy. The protected interests are under the current Convention inter alia: protection of State security, public security, suppression of criminal offences.

Comment [A60]: For logical reasons principle 12 should be placed before principle 11. The controller's obligation to inform the data subject (without the necessity of a request by the data subject) comes first in many codifications, e.g. in the GDPR or in the revised Convention 108 (Article 7bis and Article 8).

Comment [A61]: "Everyone" is imprecise.

Comment [A62]: Terminology: The document is a recommendation, not a binding legal provision!

Comment [A63]: Terminology: The document is a recommendation, not a binding legal provision! Moreover, the "obligations" reach further than the obligations contained in the revised Convention 108!

Comment [A64]: According to Article 22 § 4 of the GDPR automated decisions are, in principle, not taken on the basis of health data.

Comment [A65]: This part needs to be brought in line with Article 7bis of the revised Convention 108 and the GDPR.

The GDPR makes a difference between two situations: the data are collected from the data subject (Article 13 GDPR) and the data are not obtained from the data subject (Article 14 GDPR).

Shouldn't this be reflected here?

Comment [A66]: The word "transparency" is used only in the headline, whereas "information/inform" is used throughout the text.

Comment [A67]: Paragraph 12.3 has got nothing to do with data protection rules and with the protection of genetic data. It is a direct interference into the doctor/patient relationship. Paragraph 12.3 should therefore be deleted.

12.5. The controller does not have to provide the information where and insofar the data subject already has the information.

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

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

31. 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. When the consent is given by electronic means, proof of its expression should be made possible by any technical process.

Chapter IV. Reference frameworks of interoperability and security

32. Reference frameworks

14.1 Interoperability of systems enables to contribute to the portability of data and should for this reason be encouraged. The processing of health-related data furthermore requires that all players observe high standards to ensure the confidentiality of such data.

14.2 The development of efficient information systems, guaranteeing the respect of human rights of the data subject, aims at enhancing the health monitoring of a person during her or his treatment. To this end, health professionals as well as any public or private organisation authorised to process health-related data, in particular persons responsible for applications allowing exchange and sharing of health-related data, ~~must~~ should comply with reference frameworks to which each domestic law of a country can attribute a legally binding effect.

33. Interoperability reference frameworks

15.1 The aim of these reference frameworks is to define standards enabling the portability, exchange and sharing of health-related data by information systems and to monitor their implementation under the conditions of security required, for instance through certification schemes.

15.2 Consideration of the reference frameworks has to be integrated by design (*privacy by design*) and compliance with them is of particular importance where health-related data are collected and processed in connection with care and treatment.

34. Security reference frameworks

16.1 The processing of health-related data is to be made secure and security policies adapted to the risks for fundamental rights and freedoms must in that regard be defined.

16.2 These security rules, kept constantly 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 law should make provision for organising and regulating health-related data collection, storage and restitution procedures.

16.3 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.

16.4 Guaranteeing integrity requires verification of every action carried out on the nature of the data,

Comment [A68]: Alignment with Article 13 § 4 of the GDPR.

Comment [A69]: In accordance with Article 23 § 1 e of the GDPR

Comment [A70]: Why was this part deleted? The GDPR as well as the revised Convention 108 provide for exceptions of the right to information.

Comment [A71]: Consent is a legal basis for processing and not a right of the data subject. Of course, the data subject is free to consent to processing of her or his personal data. However, consent does not belong to the classical rights of the data subject and should therefore not be part of Chapter III (entitled: "The rights of the data subject").

Concerning sentence 2: Which right of the data subject is meant? If the controller relies on consent as the legal basis for processing, it is the controller himself who has to proof that the data subject consented to the processing (Article 7 § 1 GDPR). That means: The burden of proof is on the controller, not the data subject.

Comment [A72]: The whole chapter is not yet understandable. We therefore have a scrutiny reservation on the whole chapter and cannot accept it at the moment. The following questions need to be answered: Who is the author of these framework rules? What is the legal quality of these rules? Why shouldn't the described challenges be solved by domestic and/or international law? How is guaranteed that the legal requirements of data protection law (inter alia data security) are respected by the reference framework rules? In our opinion, reference frameworks cannot supersede the legislator. ...

Comment [A73]: Mostly the term "rights and fundamental freedoms" are used. Please align!

Comment [A74]: Terminology: The document is a recommendation, not a binding legal provision!

Comment [A75]: This is not acceptable. Who is the author of the reference frameworks? Why should even public organisations be bound by them? It has to be kept in mind that ...

Comment [A76]: What are interoperability reference frameworks? It is not possible to assess the text underneath without explaining what is meant.

Comment [A77]: What are security reference frameworks? It is not possible to assess the text underneath without explaining what is meant. ...

Comment [A78]: What does the word "these" refer to?

Comment [A79]: Maybe it is better to use the term "reference frameworks".

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.

16.5 Auditability should lead to a system making it possible to trace any access to the information system and for any action carried out by an individual to be logged to that individual.

16.6 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.

16.7 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 with appropriate measures laid down in domestic law to guarantee the confidentiality and security of the data.

Chapter V. Scientific research

35. Scientific research

17.1 The processing of health-related data for the purposes of scientific research must be carried out with a legitimate aim and in full compliance with the principles of protection of human rights applied to this particular field.

17.2 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~~.

17.3 Before consenting to the processing of his or her health-related data the data subject ~~The person concerned~~ should be - without prejudice to the recommendations laid down in Chapter III - 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 transfer 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.

17.4 As it is not always possible to fully determine ~~beforehand~~ the purpose~~s~~ of data processing for ~~different~~ scientific research purposes~~projects~~ at the time of the collection of data, data subjects should be able to give their consent 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.

17.5 Health-related data should only be used in a research project if the latter is within the scope of the ~~acceptance~~ consent, if any, given by the data subject. If the proposed use of the data in a research project is not within this scope, acceptance of the proposed use should be sought and, to this end, 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 important 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

Comment [A80]: The entire chapter needs to be carefully reconsidered. In its current version it is not acceptable. Especially the "Recommendation of the Committee of Ministers to member States on research on biological materials of human origin" needs to be carefully taken into consideration. Consistency needs to be ensured between both recommendations; "double-regulation" must be avoided. In view of the already existing Recommendation on biological materials of human origin the question should be answered whether this chapter on scientific research is needed here at all.

Comment [A81]: The requirements mentioned here are taken from the Council of Europe Recommendation on research on biological materials of human origin (biobanks) which have a much more narrowly defined scope of application, and, in Article 10 of these Recommendation, directly refer to the data subject's consent. This reference has so far been missing here, although it needs to be included in view of the broad scope (all health-related data!) and the many diverse forms of data processing which do not always take place on the basis of the data subject's consent.

Comment [A82]: Please examine whether a medical emergency can be relevant with regard to research or in the present context.

The restrictions of the data subject's rights in the context of research should not fall behind the standards set by the GDPR and its implementation at national level, (see in particular Article 89 (2) GDPR). A restriction only "in the event of medical emergency" therefore does not seem sufficient.
It should be highlighted that there is a link to the restrictions envisaged under No.11 and 12, in particular to the restriction mentioned under 11.7 in relation to the possibility under Convention 108 to introduce restrictio ...

Comment [A83]: Not necessary, since "at the time of the collection of data" defines the point of time already.

Comment [A84]: The wording "broad consent" clearly differs from the wording used in the GDPR and therefore can be misleading. In line with the GDPR, the main point here should not be the possibility to "exercise a choice", but, in the first place, to specify areas of research; after all, this is a precondition for making a choice. Therefore the wording should be brought more in line with recital 33 of the GDPR.

Comment [A85]: Why is the word "acceptance" introduced and what exactly does it mean? So far, the term "consent" has been used in the text. The Recommendations on research on biological materials of human origin use the words "consent or authorisation".

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

17.6 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.

17.7 Healthcare professionals who are entitled to carry out their own medical research and scientists in other disciplines should, on the basis of the relevant legal grounds, 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 17.3~~.

17.8 Pseudonymisation of the data, with intervention of a trusted third-party at the separation stage of the identification, is among the measures that can be implemented to safeguard the rights and fundamental freedoms of the data subject. This should be preferred 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.

17.9 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 and the data subject should be informed accordingly.

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

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

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.

36. Mobile applications

18.1 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 social provision and/or are processed in a medical context, they constitute health-related data. In this connection they should 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 ~~of States~~.

18.2 Persons using such mobile applications, as soon as they involve the processing of their personal data, must enjoy similar rights to 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 terms and conditions 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.

18.3 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.

18.4 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.

Comment [A86]: We have considerable reservations regarding 17.5:

17.5 is an - incomplete - repetition of Article 21 (1) and (2) of the Recommendations of the Council of Europe on research on biological materials of human origin, despite the fact that the situation regarding all health-related data is not completely comparable. This selective copying gives rise to further questions.

Among other points, it should be made clear that in this context one cannot categorically take the consent of the data subject for granted, unlike in the area of biobanks.

In addition, in contrast to the Recommendations on biobanks, the current draft does not distinguish between identifiable and non-identifiable materials. Whether, in view of the broad scope of the Recommendations on health-related data, we can do without this differentiation is something that still needs to be examined.

On the whole, 17.5 needs to be thoroughly re-examined against the backdrop of the GDPR's requirements and systematics regarding data processing for research purposes (in particular Article 5 (1) b), Article 9 (2) j), Article 89 (2) GDPR).

Comment [A87]: Even in such cases, however, there should be rules for deletion.

Comment [A88]: We support the concept of pseudonymisation as an important safeguard. It should be added, however, that - if the purpose can be reached even by anonymization of the data - anonymization is preferable.

Comment [A89]: It is necessary to regulate in detail that research results obtained with the data subject's data up to that point do not have to be deleted. Otherwise, by withdrawing from a research project at any point in time, for example even shortly before the end of a study, the data subject could render the results obtained up to then completely worthless.

Comment [A90]: Please chose one version for the entire text: It seems that mostly the term "rights and fundamental freedom" is used.

Comment [A91]: Why are these words necessary here?

Comment [A92]: Why should there be a difference?

IRELAND / IRLANDE

Draft Recommendation on the Protection of Health-Related Data

Ireland's Comments

General
The terminology used should reflect the fact that this is a recommendation e.g. use "should" and not "must" or "shall".

Chapter I
Scope (Article 1)
We would like to add "and voluntary" after "public" to take account of our health system where we have public, private and voluntary hospitals.

Definitions (Article 2)
It is suggested that the definitions should be consistent with those in draft modernised Convention 108 and the GDPR (Regulation (EU) 2016/679).

Chapter II
Principles concerning data processing (Article 4)
Would it be possible to amend this heading as the text includes the standard data protection principles as set out in Article 5 of the GDPR and other requirements. Perhaps the heading used in the modernised Convention 108 "legitimacy of data processing and quality of data" could be used.

Paragraph 1
It is suggested that the text of point (b) should make it clear the safeguards should be set out in national law and not left exclusively to the decision of individual archivists, researchers or statisticians to decide what is appropriate.

It is suggested that the following text be added at the end of point (c):
Further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health may be set out in national law. (See article 9.4 of the GDPR)

Paragraph 4
It is suggested that the following text should be added to the end of paragraph 4:
"except where explicitly provided for in domestic law".

Paragraph 5
It is suggested that the introduction be amended to read as follows:

Health-related data may be processed for the following purposes where such processing is foreseen, and appropriate safeguards are provided, in law:

Data concerning unborn children (Article 7)
It is suggested that this is a matter that should be left to national law.

Genetic Data (Article 7)
It is suggested that the recommendation should provide that genetic data cannot be sold for any purpose.

Shared medical secrecy for purposes of providing and administering care (Article 8)
It is suggested that "except as explicitly provided for in law" should be added after "health-related data".

Storage of health-related data (Article 10)
Delete "not" in the phrase "must not be stored" in paragraph 1.

Chapter III
The right of access, objection, rectification, erasure and portability (Article 11)
This article should be brought into line with the GDPR.

Transparency (Article 12)
This article should be consistent with the GDPR.

Paragraph 1
The words "must" and "should" should be replaced with "should" and "may" respectively.

The need to provide details of the processor is not clear.

It may not be possible to specify the 'length of conservation' of the personal data; if this provision is to be retained, it is suggested that the text should state "the period for which the personal data will be stored, or if this is not possible, the criteria used to determine that period".

Is it realistic to expect that a data subject should be given information in relation to the "specific techniques used to process their health-related data"?

Paragraph 3
This paragraph doesn't appear to be relevant to data protection.

Additional paragraphs
It is suggested that paragraphs should be added:
- to provide that it is not necessary to provide the information referred to above where the data subject already has it; and
- to provide for some restrictions where provided for by law similar to article 11.7.

Consent (article 13)
The meaning of the second sentence of this article is not clear.

Chapter IV
Reference Framework (Article 14)
Would it be possible to clarify the meaning of "players".

Chapter V
This chapter requires careful consideration.

Scientific research (Article 17)
It is suggested that this paragraph should be redrafted to provide that explicit consent is the default position of use/further processing/disclosure of personal health data for research purposes except in those circumstances where domestic law provides otherwise.

Paragraph 9
This paragraph should be redrafted to clarify that withdrawal of consent doesn't affect research already carried out.

THE NETHERLANDS / PAYS-BAS

Comments of “The Netherlands”

The Netherlands proposes with a view to a balanced approach of the protection of health related data and the need for the processing of these data in the context of, under exceptional circumstances, public security (amongst other legitimate grounds mentioned in to the Convention 108 on the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 1981) the following:

- It firstly wishes to take on board a *general* reference to the Convention 108 in the recitals on page 2. Article 8 of the ECHR has been mentioned there, but the Convention is an important elaboration of article 8 of the ECHR. Its mention cannot be missed here.

- Second, the Netherlands wants to see a more explicit reference to article 9 (on the exceptions) of the same Convention 108 in both principle 9 or 9.3, and 11 or 11.1 of the concept Health Recommendation. This is in order to secure the Council of Europe legal framework that under some circumstances health data can be lawfully communicated to recipients that are authorized by domestic law to have access to the data and that there are circumstances that justify a refusal of the right of the individual to be informed about the data that are processed about him. In our perspective, the recommendation cannot go without mentioning the legitimate exceptions.

PORTUGAL

L'expression "maintenu à l'état de l'art" doit être clarifiée en ce qui concerne la responsabilité de ce maintien « à l'état de l'art ». Qui prend cella en charge, les gouvernements, la communauté scientifique / médicale?

La réponse que nous proposons ? Les deux. L'investigation scientifique médicale dans le cadre de son normatif spécifique (notamment de nature éthique) et l'État, notamment dans le cadre des politiques de santé publique, entre autres.

Peut-être à répondre dans le cadre du rapport explicatif.

La phrase « Elle recouvre des formes diverses comme les objets connectés et les dispositifs médicaux qui peuvent notamment être utilisés à des fins diagnostiques, thérapeutiques ou de bienêtre. » semble contenir une dichotomie, or cela n'est pas correcte, où au moins pas toujours correcte.

On propose que la phrase soit modifiée de la façon suivante : « Elle recouvre des formes diverses comme les objets connectés y inclus les dispositifs médicaux qui peuvent notamment être utilisés à des fins diagnostiques, thérapeutiques ou de bienêtre. »

Explication: il n'y pas, a notre avis, une alternative. En effet certains dispositifs interconnectés sont des dispositifs médicaux, d'autres ne mérite pas cette classification, mais les données gérés par eux peuvent être utiles pour les diagnostiques. Ce serait le cas notamment de certains dispositifs utilisés par les sportifs, et d'autres d'utilisation domestique.

Peut-être que dans le Rapport Explicatif il devrait être clarifié si et dans quelle mesure les Parties s'engageront à reconnaitre les professionnels de santé d'une autre Partie. Même en sachant qu'une Recommandation n'est pas un instrument de Droit International avec la portée d'une Convention.

On suggère de remplacer "devraient" par "doit".
Tout 'en s'agissant d'une Recommandation là matière en question requiert qu'une obligation d'agir un plus forte soit imposée aux Parties.
En plus le mot « doit », en Anglais « must » est utilisé ailleurs dans cette même Recommandation.

A notre avis, les situations auxquels se réfèrent les paragraphes b), c) et d) du numéro 17.5, peuvent justifier une divulgation limité a certain destinataires (autorités scientifiques ou autres) dans le cadre de la recherche, si une loi où contrat l'impose, même dans ce cas. On suggère que cela soit clarifié dans le Rapport Explicatif et, où, même ajuté au texte de la Recommandation.

SWEDEN / SUEDE

Comments on the Draft Recommendation of the Protection of Health Data

The Swedish position

Sweden's position is that since there are many remaining questions concerning the Recommendation and the implementation of the EU Regulation 2016/679 General Data Protection Regulation it would be difficult for Sweden to support the adoption of the Recommendation at this point. The reason for the position is commented below.

General comments

The protection of personal data is a fundamental right but it may, in certain circumstances such as the protection of health, be balanced in accordance with laws necessary in a democratic society. The processing of health data is important for various stakeholders such as patients, health care personal and scientists. Sweden’s position regarding data for the purposes of scientific research is the same as the EU policy, that the data should be as open as possible, and as closed as necessary. The Recommendation covers processing of personal data that are also regulated in the new EU Regulation 2016/679 General Data Protection Regulation. The process of implementing the General Data Protection Regulation in the health sector is still ongoing in Sweden. Before the national implementation is finalized, it is premature to adopt the Recommendation. Therefore, at this time, it would be difficult for Sweden to support the adoption of the Recommendation. It is important that the Recommendation and the EU Regulation can coexist without problems for those who need processing health data.

SWITZERLAND / SUISSE

- Nous saluons sur **le principe** la volonté de clarifier et d'adapter la recommandation existante (N°R (97) 5 aux enjeux posés par l'évolution technologique et l'informatisation croissante du secteur de santé pour la protection des données de santé.
- Dans la version française, il serait bien de revoir ou d'introduire la numérotation des différentes dispositions.

- **Objet**: Concernant **les objectifs** de la recommandation, nous saluons le fait que, dans la version anglaise, à côté de la protection des données et le respect des droits et des libertés fondamentales le point 1 « *objet*» mentionne explicitement un autre objectif essentiel pour les autorités de santé: celui de l'utilisation des données de santé à des fins d'amélioration de la qualité et d'efficacité des soins de santé et des systèmes de santé. En revanche, cette mention fait défaut dans la version française qui devra donc être complétée pour correspondre à la version anglaise*: "It also highlights to this end the importance of developing interoperable and secured information systems* ***in a manner enabling the quality of care and the efficiency of health systems to be enhanced***".

- **Définitions**: Au niveau des **définitions**, nous soulignons un risque de contradiction entre, d'une part, la définition « *donnée à caractère personnel* », qui souligne - à juste titre - que les données sont dites anonymes lorsqu'une personne n'est pas identifiable. Si l'identification requiert des moyens/délais déraisonnables, les données sont considérées comme anonymes. D'autre part, sous l'expression « ***l'anonymisation*** », on parle des personnes ne pouvant *« plus être identifiée ni directement ni indirectement* ». Or, nous savons que l'anonymisation n'est presque jamais totalement irréversible. L'anonymisation ne signifie souvent plus une impossibilité absolue de réidentification, mais le fait que celle-ci ne peut intervenir sans moyens disproportionnés. Par conséquent, il nous semblerait adéquat de préciser également sous la définition d'anonymisation que si l'identification (directe ou indirecte) requiert des moyens ou des délais déraisonnables les données sont toujours considérées comme anonymes.

- **Définition de pseudonymisation** : nous proposons de mettre donnée au pluriel : « … des données non identifiantes … »

- **Définition de données génétiques:** Il conviendrait de clarifier si la définition couvre aussi des aspects ne se référant pas à la santé (origine de personnes déterminées, tests de comportement, talent sportif). Les experts suisses consultés marquent une préférence pour une définition qui reprenne ou se rapproche de celle du règlement européen.

- **4.1 b:** Les finalités sont définies au principe 5, faut-il conserver cette disposition ? Si oui, nous proposons de la modifier comme suit :

  Les données doivent être collectées pour les finalités énoncées au principe 5 et ne doivent pas être traitées de manière incompatible avec ces finalités.

- **5.1 b**: nous proposons de mettre les exemples dans le rapport explicatif.

- **5.1 d** : qu'entend-on par motif d'intérêt général ? S'agit également d'un motif d'intérêt public. Si oui, déplacer « domaine de gestion des demandes de prestation … » dans le principe 5.1 b

- **5**.1. e : la finalité compatible est mentionnée au principe 4.1 b. Nous proposons de biffer la lettre e

- **5**.1 f : mettre le passage entre ( ) dans l'exposé des motifs.

- **5**.2 : ne faudrait-il pas intégrer le principe 13 dans le 5.2 ?

- **5**.4 : ce principe ne fait-il pas double emploi avec le principe 16 ?

- **7.2 et 7.3:** L'interdiction d'utiliser les données génétiques pour d'autres finalités que celles prévues aux chiffres 7.2 et 73 paraissent trop restrictives aux yeux des experts suisses consultés. Le droit suisse (de lege lata et de lege ferenda) n'interdit pas des analyses

génétiques à des fins non médicales (par exemple détermination ethnique, test de paternité, tests de comportement, etc.).

- **7.5**: Nos experts estiment que de faire dépendre le traitement de ces données d'une évaluation indépendante est trop limitatif. La porte devrait demeurer ouverte pour d'autres critères équivalents.
- **7.6:** Il est proposé de prévoir que le droit interne puisse limiter le droit de savoir des personnes vulnérables. En Suisse, la loi restreint ce droit en relation avec les personnes incapables de discernement et les enquêtes prénatales. En particulier, il ne faut pas pouvoir communiquer des informations dont l'obtention nécessiterait per se une analyse illicite.
- **8:** Le droit suisse ne connaît pas de secret médical partagé. La communication de données du patient entre personnel de santé ne peut se faire qu'avec le consentement des personnes concernées. Ainsi le droit d'opposition (8.1) est insuffisant; il faut prévoir le consentement explicite.
- **11.4:** le droit à la portabilité est certainement important. Toutefois la rédaction du principe devrait être revu. Nous proposons la formulation suivante : *« La personne concernée devrait, dans les limites du droit interne, se voir reconnaître un droit à la portabilité de ses données lui permettant d'exiger du responsable du traitement … »* .
- **11.**7 mettre la fin de la phrase « dont notamment … » dans le rapport explicatif.
- **12** : **Le droit à l'information** - Il nous paraît difficile, notamment pour les établissements de soins, de donner systématiquement une information aussi exhaustive que prévue par cette disposition au moment de la collecte des données. Dans le rapport explicatif, il faudrait en tenir compte et expliciter ce que l'on entend par « information appropriée et adaptée » (12.2)
- **14**.2 (14.1 dans la version anglaise) nous proposons de biffer ce principe et de le mettre dans le rapport explicatif. S'il devait être maintenu, il faut rajouter à la fin de la deuxième phrase de la version française « données ».
- **15**.1 Ce principe appartient au chapitre sur les définitions. Il pourrait aussi être placé dans le rapport explicatif.
- **16**.6 Ce principe n'apporte pas de valeur ajoutée et il pourrait être biffé.
- **17** Nous nous demandons s'il ne serait pas indiqué, vu la complexité des questions relatives à la recherche scientifique, d'élaborer une recommandation spécifique sur le sujet.
- **17.1** Nous proposons soit de biffer la dernière partie de la phrase, soit de remplacer « protection des droits de l'Homme » par « respect des droits et des libertés fondamentales »
- **17.7**: Cette disposition est peu claire. Postule-t-on la possibilité d'utiliser les données de santé sans le consentement de la personne concernées ou introduit-on indirectement un simple droit d'opposition. Le droit suisse est plus strict et exige dans la plupart des cas le consentement. La recommandation devrait au moins permettre au droit national d'être plus restrictif.
- **17.9**: L'exigence de détruire ou d'anonymiser les données lors d'un retrait de la recherche peut être en contradiction avec la nécessité de bonnes pratiques cliniques, resp. du droit européen (règlement sur le Clinical Trial). Cela nécessite de pouvoir conserver l'ensemble des données, év. sous une forme pseudonymisée (protection contre les biais, les falsifications, etc.).

UNITED KINGDOM / ROYAUME-UNI

Para 17.4
Is this time limited? What about if data has been used and they wish to remove it post hoc? This could impact on the analysis and / or the interpretation of results.

Para 17.5
Who defines what is reasonable in these circumstances?

Para 17.9
Is that only during the research period? How long afterwards can they make this request? Is there a time limit?

ASSOCIATION EUROPEENNE POUR LA DEFENSE DES DROITS DE L'HOMME /
EUROPEAN ASSOCIATION FOR THE DEFENSE OF HUMAN RIGHTS (AEDH)

PROJET DE RECOMMANDATION EN MATIERE DE
PROTECTION DES DONNEES RELATIVES A LA SANTE

Page 15 Concernant les dispositifs mobiles

Chapitre VI. Les dispositifs mobiles
Les dispositifs mobiles permettent le développement de nouvelles pratiques médicales et de santé publique. Ils recouvrent tout à la fois des applications concernant le mode de vie et le bien-être qui peuvent se connecter à des dispositifs médicaux ainsi que des systèmes de conseil personnalisés et d'observance.

Il nous semble qu'il est nécessaire d'ajouter les objets connectés qui ne sont pas des dispositifs médicaux mais qui sont bien cités dans la définition des applications mobiles page 6 *(- L'expression « applications mobiles » désigne un ensemble de moyens accessibles en mobilité permettant de communiquer et de gérer des données relatives à la santé à distance. Elle recouvre des formes diverses comme les objets connectés et les dispositifs médicaux qui peuvent notamment être utilisés à des fins diagnostiques, thérapeutiques ou de bien-être.)*

Ce qui donnerait :
Chapitre VI. Les dispositifs mobiles
Les dispositifs mobiles permettent le développement de nouvelles pratiques médicales et de santé publique. Ils recouvrent tout à la fois des applications concernant le mode de vie et le bien-être qui peuvent se connecter à des objets connectés, des applications de santé reliées à des dispositifs médicaux ainsi que des systèmes de conseil personnalisés pour la santé et d'observance de traitement.

INTERNATIONAL CHAMBER OF COMMERCE (ICC) / CHAMBRE INTERNATIONALE DU COMMERCE (CIC)

ICC comments on Council of Europe recommendation on the protection of health data

The International Chamber of Commerce (ICC) is the world business organization and works to further the development of an open world economy with the firm conviction that international commercial exchanges are conducive to both greater global prosperity and peace among nations. Consisting of over six million companies, chambers of commerce and business associations in more than 100 countries ICC has vast experience providing business expertise to policy-makers globally.

ICC's Commission on the Digital Economy develops policy positions and practical tools for the Internet and information communications technology (ICT). The Council of Europe "*Draft recommendation on the protection of health data"* provides principles for the exchange and sharing of health data by means of digital tools and raises important factors which would benefit from cross-sectoral business experience and expertise. Through these comments ICC would like to highlight the societal benefits of emerging technology and share perspectives on the importance of balanced, flexible, multistakeholder approaches to managing the privacy and security implications of their use.

The Council of Europe is both justified and timely in developing guidance related to health data. Data is used and exchanged at ever-increasing levels and data flows are increasingly being recognized as catalyzing economic efficiency and productivity, raising welfare and standards of living. Preventative healthcare offers immense opportunities for health-care providers and systems by predicting disease, developing treatments, providing greater efficiency and freeing up scarce resources, for the treatment and benefit of patients. Carefully balancing opportunities to realize the benefits of technology for health-systems and ensuring effective security, privacy and confidentiality of personally identifiable patient information is therefore of increasing importance.

With regard to the current Recommendation draft text, however, ICC would like to highlight that the Council of Europe does not amply explain the use of technology for societal benefit particularly with regard to health, and its role in development. The Council of Europe misses an opportunity to empower professionals to use and further innovative use of technologies and practices in ways that serve society while ensuring the effective security, privacy and confidentiality of personally identifiable information.

While the recitals now to a limited extent make reference to beneficial uses of data, ICC suggests including more explicit statements to highlight the importance of applying technology and safeguarding privacy in the sharing and use of health and medical data for societal benefit. Health is arguably as much of a fundamental right as privacy. Without this wider and future-oriented frame, the possible "lost opportunity" in health care if technology is not applied or innovated may have fatal consequences for patients and future generations. Health and privacy are too often seen as competing concepts but this does not have to be the case. Indeed similarly to other sectors, there are many opportunities to optimize health systems across innovative use of data and ensure the protection of personal data and health care rights.

The Council Europe correctly identifies the use and benefit of electronic medical records as well as the growing importance of medical applications and those applications that may track data potentially related to medical data; fitness "wearables" etc. ICC underscores that it is challenging to provide guidance for an emerging set of products, as their role and use can be unclear. For example, in Seattle a team of orthopedic surgeons started sending patients home with a gaming console because of its ability to track motion which allowed patients to evaluate their range of motion in physical therapy. A gaming console would arguably not be considered a medical device, but the innovative use of non-medical technology, allowed the practice to optimize patient visits assuring that those making good progress could continue at home and those not progressing could be called into the surgery. The use of technology resulted in fewer patient visits, greater patient satisfaction, better patient outcomes and cost savings to both the practice and insurance.

The importance of flexibly is especially true for emerging technologies such as cloud, big data and the Internet of things.[1] While these concepts are well known, current uses are only beginning to understand and exploit their true potential.

The Council of Europe recently prepared guidance related to big data and we reference the ICC comments on same. Big data models are predicated on the ability to associate streams of data from varied and often fast changing, real-time sources. Associated correlations across data may yield insights that lead researchers to ask new questions of potential significance. For example, in the case of health this could lead to new treatments of disease. Those correlations give rise to the potential purpose for which the data may be beneficially used and may fuel the following questions: How can one provide a specific and explicit consent when the use of information may not be known? Do we forgo the potential benefits of innovation? Is the missed innovation that would benefit a fundamental right (for example health) transferred into an opportunity cost to society?

The Council of Europe recommendation contains inferences which can be expanded into a possible solution path. Section 4.1b introduces the concept of compatible processing for historical, scientific and statistical purposes "on condition that additional guarantees apply". Section 17.3 includes the possibility of practitioners using collected medical health data for unspecified compatible future research as long as the data subject has been informed of, and not objected to, the possibility. These could become the building blocks for a more flexible approach. Additional guarantees could be developed to assure that appropriate and validated security and privacy protocols are in place with appropriate sharing limitations. This may permit the use of more generalized purpose specifications with flexibility for future innovative use while enabling data subjects such as patients to feel confident about the circumstances of the processing. Similarly where previously information was collected with only a specific and limited consent, more compatible uses of information for research purposes may be found where the lack of new individualized consent is replaced by appropriate ethical review. This review would be compliant with established research norms in the relevant sector such as a health, and consider appropriate stakeholder interests and expertise.

While the Council of Europe recommendation may not specifically preclude such explorations, the opportunity to enter into constructive discussions of what such a framework might look like and what it could accomplish should be encouraged. Furthermore, a risk particularly penitent to the health community related to privacy is developing where researchers are limiting their scope of innovation from a fear of privacy transgression or overwhelming administrative burden. ICC encourages a dialogue that results in both enhanced innovation and privacy.

As an observer of the Council of Europe, ICC would like to thank the Council of Europe for considering these comments and remains available to work with the Council of Europe as it continues to define practical, optimally effective guidance on the protection personal data.

About The International Chamber of Commerce (ICC)

The International Chamber of Commerce (ICC) is the world's largest business organization with a network of over 6 million members in more than 100 countries. We work to promote international trade, responsible business conduct and a global approach to regulation through a unique mix of advocacy and standard setting activities—together with market-leading dispute resolution services. Our members include many of the world's largest companies, SMEs, business associations and local chambers of commerce.

www.iccwbo.org@iccwbo

[1] https://iccwbo.org/publication/icc-policy-primer-on-the-internet-of-everything/