COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 3 October 2016

T-PD(2016)04rev2

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

DRAFT RECOMMENDATION ON THE PROTECTION OF HEALTH DATA

Directorate General Human Rights and Rule of Law

Recommendation

Appendix to the Recommendation

Chapter I
General provisions

Chapter II
The legal conditions for the use of health data

Chapter III
The rights of the individual

Chapter IV
Reference framework for the processing of health data

Chapter V
Research in the health field

Chapter VI
Mobile applications

Recommendation CM/Rec(2017)…. of the Committee of Ministers to member States on the protection of health 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 data, which now takes place in an environment that has changed considerably since the adoption of Recommendation No. R (97)5 on the protection of medical data.

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

People's desire to have more control over their data and to control the way in which their data are processed 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 their treatment.

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 No. R (97) 5 on the protection of medical data, with the more general term "health data" being preferred, while reaffirming the sensitivity of health data and the importance of regulating their use so as to guarantee due regard for the rights and fundamental freedoms of the individual, in particular the right to privacy.

Health data are among the data belonging to a particular 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 to the risk of discrimination resulting from irregular processing.

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

- take steps to ensure that the principles set forth in the appendix to the present Recommendation, which replaces Recommendation No. R (97) 5 mentioned above, are reflected in their law and practice;
- ensure, to that end, that the present Recommendation and its appendix are brought to the attention of data protection officers of the authorities responsible for healthcare systems, with the latter being responsible for ensuring their transmission to the various actors who process health data, in particular healthcare professionals;
- 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 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 data in order to guarantee respect for the rights and fundamental freedoms of every natural person, 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 provides guidelines for developing interoperable and secured information systems in a manner enabling the quality of care and the efficiency of health systems to be enhanced.

2. Scope

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

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

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

3. Definitions

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

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

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

- The expression “pseudonymisation” refers to a technique 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 manner and which would make identification possible. Pseudonymised data are personal data.

- The expression “health 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 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 process or set of processes performed on personal data, such as collection, recording, storage, alteration, extraction, communication, provision, deletion or destruction of data, or the application of logical and/or arithmetical processes to these data.

- The expression “data controller” means the individual or legal entity, public authority, service, agency or any other organisation which, on its own or jointly with others, has the power to take decisions concerning 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 identification, interoperability and security.

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

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

- The expression "right to portability" denotes a person's right to receive data concerning them that have been provided to a data controller, where the processing is based on the consent of the data subject or on a contract, in a structured, commonly used format, and to transmit them, if necessary, to another controller. This right is made possible by the interoperability of the formats used by the information systems.

- The expression "mobile applications" denotes a set of means accessible in a mobile environment making it possible to communicate and manage health data remotely. It covers different forms such as connected medical objects and devices 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 "health data hosting" denotes the use of external data hosting service providers for the secure and lasting storage of health data on the Internet.

Chapter II

The legal conditions for the processing of health data

4. Principles concerning data processing

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

a. Personal data must be processed in a transparent, legal and fair manner.

b. Personal data must be collected for explicit, specific and legitimate purposes 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 enable human rights and 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 free, specific, informed and unambiguous consent of the data subject or on other legitimate basis laid down by law.

d. Health data must, in principle, be collected from the data subject. They cannot be collected from other sources except in accordance with principles 5, 6, 7, 9 and 12 in this recommendation, provided that this is necessary to fulfil the purpose of the processing or if the data subject is unable to provide the data.

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

f. The data must not be stored in a form allowing identification of the data subjects for a period which exceeds that 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 guarantees enable human rights and freedoms to be respected.

g. Appropriate security measures, taking into consideration the latest technological developments, the sensitive nature of health data and the assessment of potential risks based on reference frameworks, should be established to prevent risks such as accidental or unauthorised access to personal data or the destruction, loss, use, modification or disclosure to unauthorised persons of those data.

h. The rights of the person whose data are collected and processed must be respected, particularly the rights of access to the data, information, rectification, objection, deletion and portability.

4.2 The processing of health data is permissible only insofar as appropriate guarantees are provided in domestic law, supplementing those in Convention 108 to prevent any risk to the interests, rights and fundamental freedoms of the data subject which the processing may represent, in particular the risk of discrimination.

4.3 Data controllers and their processors who are not health professionals should only collect and process health data in accordance with the same rules of confidentiality and security measures that apply to health professionals.

5. Purpose of processing health data

5.1 Health data may be processed and communicated:

a. if provided for by law or if the processing is based on a contract entered into with a health professional which stipulates appropriate guarantees:

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

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

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

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

   or

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

or

c. insofar as this is authorised by law, in particular:

i. for the purpose of safeguarding the vital interests of the individual, or the data subject or another person;

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

iii. for reasons essential to the recognition, exercise or defence of a legal claim;

iv. for reasons relating to scientific research in the biomedical field and the medico-social sector;

v. for processing for statistical, historical or scientific research purposes under the conditions defined by domestic law in order to guarantee protection of the data subject's legitimate interests and where the individual cannot be identified from the published result.

In all cases, suitable 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.

5.2 Additional obligations

a. These personal data protection principles must be taken into account and incorporated right from the design of information systems which process health 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.

b. 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

6. Medical data concerning unborn children, inter alia such as data resulting from a preimplantation diagnosis, should enjoy a protection comparable to the protection provided to health data of a minor.

7. Genetic data

7.1 Genetic data processed with a preventive aim, for diagnosis or for treatment of the data subject or a third person or for scientific research should be used only for these purposes or to enable the data subject to take a free and informed decision on these matters.

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

7.3 Any processing of genetic data other than in the cases provided for in paragraphs 7.1 and 7.2 should only be carried out where prescribed by law. The processing of genetic data for predictive purposes, to identify the subject as a carrier of a gene responsible for a disease or to detect a genetic predisposition or susceptibility to a disease can only be performed for health purposes or for scientific research linked to health purposes, and subject to appropriate safeguards provided for by law.

7.4 The data subject is entitled to know any information collected about his or her health. However, the person subjected to genetic analysis should be informed, prior to such analysis, of the possibility he or she has not to be informed of unexpected findings. His or her wishes not to be informed may, in his or her interests or in the interests of a concerned third party, have to be restricted.

7.5 The publication of genetic data which would identify the data subject, a consanguine or uterine relative of the data subject, a member of his/her [social] family or a person who has a direct link with his/her genetic line, should be prohibited, except where expressly prescribed by law with the necessary safeguards.

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

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

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 should recognise a shared professional secrecy, between professionals who are themselves legally bound by such secrecy.

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

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

9. Communication to authorised third parties

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

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

9.3 Medical officers of insurance companies and employers cannot, in principle, be regarded as third parties authorised to have access to the health data of patients unless domestic law makes provision for this with appropriate safeguards.

10. Storage of health data

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

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

Chapter III

Rights of data subjects

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.

11. Right to information

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

They must be informed of:

- the identity and contact details of the controller and of the processors where relevant,
- the purpose for which the data are processed, and where appropriate of the relevant legal basis for it,
- how long the data will be stored, or, if possible, the criteria used to determine this period,
- 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, or of withdrawing their initial consent, and the implications of such withdrawal,
- 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 of deletion of their health data, and the possibility of objecting to the processing thereof,

They should also be informed:

- that their data may subsequently be processed for a compatible purpose, in accordance with appropriate safeguards provided for by domestic law,
- of the specific techniques used to process their health data,
- of the possibility of loging a complaint with a supervisory authority,
- of the existence of automated decisions, including profiling.

11.2 This information should be provided at the time of data collection or of the first communication, unless it proves impossible or requires disproportionate efforts, in particular for processing for the purposes of scientific or historical research 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 him/her. If a legally incapacitated person is capable of understanding, he/she should be informed before his/her data are processed. Only urgency or the impossibility of providing information can give rise to an exemption from the obligation to provide information; care takes precedence over information.

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

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

12. Consent

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

13. Rights to access, objection, correction, deletion and portability

13.1 Everyone has the right to know whether personal data which concern them are being processed, and, if so, to have access 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 period for which their data will be stored, or, if possible, the criteria used to determine this period
- that they have the possibility, if applicable, to object to the processing of their data or revoke the consent that they initially gave

- the fact that they can make a complaint to a supervisory authority,
- the existence of automated decisions which include profiling.

13.2 The right of access to information, on paper as well, enables the data subject to exercise his/her right of rectification and deletion and the right to obtain data in a structured format which, when the automated processing is based on consent or a contract, makes it possible to transmit them to another controller designated by the data subject.

13.3 The right of deletion is exercised subject to the cases prescribed by law and invoking legitimate grounds. The data subject is entitled to object on grounds relating to his/her personal situation to the collection of his/her personal health data, unless it is anonymised or unless the person holding the data invokes an overriding and legitimate reason concerning the public interest of public health.

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

Chapter IV

Reference frameworks for the processing of health data

In the processing of health data all players should observe high standards to ensure the confidentiality of health data.

14. Reference frameworks

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

15. Interoperability reference frameworks

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

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

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

15.4 They are based on the following principles.

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

b) using interoperable services and common rules on use;

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

d) guaranteeing data subjects reliable identification to ensure the uniqueness of their identity within the different information systems.

e) ensuring authentication of the persons and systems involved in the processing of the data;

f) using secure solutions as defined in Principle 16.

16. Security reference frameworks

16.1 The processing of health data should be made secure.

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

16.3 System availability – i.e. the proper functioning of the system – 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 servers 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 storing health data in analogue and digital systems 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 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 use of health 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 in the fields concerned.

17.2 The need to use health data should be evaluated in the light of the aim pursued.

17.3 Prior to consent to the use of health data for the purposes of scientific research, the person concerned should be provided with comprehensible information that is as precise as possible with regard to:

– the nature of the envisaged research and the possible choices that he or she could exercise;

– 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 his or her right to refuse to consent and to withdraw it at any time. Restrictions may be applied in the event of a medical emergency. Data subjects should be able to give their consent solely for certain fields of research or certain parts of research projects, insofar as the desired goal allows this.

17.4 The conditions in which health data are processed for scientific research must be assessed by the body or bodies designated by domestic law.

17.5 Healthcare professionals who are entitled to carry out their own medical research and scientists in other disciplines should be able to use the health data which they hold as long as the data subject has been informed of this possibility beforehand and has consented to it.

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

17.7 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

18. Mobile applications

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

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

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