COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 9 May 2016

T-PD(2016)04rev

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

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

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

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

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

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

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

- ensure that the principles set forth in the appendix to the present Recommendation, which replaces Recommendation No. R (97) 5 mentioned above, are reflected in the implementation of national legislation on protection of health data, as well as in other branches of any law on the use of health data;
- ensure, to that end, that the present Recommendation and its appendix are brought to the attention of the authorities set up under national data protection legislation to monitor the application of that legislation, as well as of the authorities responsible for healthcare systems;
- promote acceptance and application of the principles set forth in the appendix to the present Recommendation, using additional instruments such as codes of conduct, while ensuring that these principles are well-known, understood and applied by all the players in the healthcare sector and taken into account in the design, deployment and use of the ICTs in that sector.

Appendix to Recommendation CM/Rec(2016)…

Chapter I

General provisions

1. Purpose

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

2. Scope

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

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

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

3. Definitions

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

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

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

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

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

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

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

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

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

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

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

- The expression "anonymisation" denotes the process applied to health data so that the data subject

can no longer be identified, either directly or indirectly. Anonymisation is irreversible.

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

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

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

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

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

Chapter II

The legal conditions for use of health data

4. *Privacy by design*

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

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

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

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

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

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

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

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

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

4.4 In principle, health data must be collected and processed by health professionals, agencies acting under the responsibility of health professionals or by the data subjects themselves. Data controllers

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

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

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

5. Processing of health data

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

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

5.3 Health data may be processed and communicated:

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

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

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

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

6. Data concerning embryos and foetuses

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

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

7. Genetic data

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

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

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

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

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

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

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

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

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

9. Communication to authorised third parties

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

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

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

10. Storage of health data

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

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

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

Chapter III
The rights of the individual

11. Right to information

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

They must be informed of:

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

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

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

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

11.4 A person's wish to be kept in ignorance of a diagnosis or prognosis should be complied with, except where third parties run a risk of transmission. In a medical emergency, when the person's life is at stake, care takes precedence over information.

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

12. Consent

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

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

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

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

13. Right of access, objection and portability

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

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

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

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

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

a. this constitutes a necessary and appropriate measure in a democratic society in the interests of protecting national security or public safety, or of preventing, investigating or punishing criminal offences; or
b. knowledge of the information is likely to cause serious harm to the data subject's health; or
c. the information on the data subject also reveals information on third parties or if, with respect to genetic data, this information is likely to cause serious harm to a consanguine or uterine relative or to a person who has a direct link with this genetic line; or
d. the data are used for scientific or historical research purposes or statistical purposes where there is no identifiable risk of an infringement of the rights and fundamental freedoms of data subjects, in particular where such data are not used for decisions or measures relating to a specific individual.

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

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

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

Chapter IV

Reference frameworks for the processing of health data

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

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

14. Reference frameworks

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

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

15. Interoperability reference frameworks

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

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

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

15.4 They are based on the following principles.

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

b) using interoperable services and common rules on use;

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

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

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

data by means of arrangements which all operatives recognise and are such as to guarantee security in the exchange and sharing of the data;

f) using secure solutions as defined in Principle 16.

16. Security reference frameworks

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

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

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

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

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

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

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

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

17. Health data management services

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

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

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

The information in this medical file may be shared, with the patient's consent, by professionals involved in care provision for the patient in the conditions defined in paragraph 8.1.
17.3 Any electronic messaging system permitting the exchange of personal health data must comply with the reference framework defined in section 14.

Chapter V - Research in the health field

18. Research in the health field

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

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

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

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

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

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

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

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

Chapter VI – Mobile applications

19. Mobile applications

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

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

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