COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

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

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.

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 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 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.

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 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.

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

9. Communication to 'authorised recipients'

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.

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.

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, 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.

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.

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 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 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 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 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.

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.