COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 8 June 2018 T-PD(2018)06

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

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

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

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

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

This changed environment is due to the phenomenon of data digitisation, made possible by the growing computerisation of the professional sector and particularly of activities relating to health care and prevention, to life sciences research and to health system management and to the proliferation of exchanges of information arising from the development of the Internet.

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

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

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

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

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

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

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

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

- take steps to ensure that the principles set forth in the appendix to this Recommendation, which replaces Recommendation (97)5 above-mentioned, are reflected in their law and practice;

- ensure, to that end, that this 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 this Recommendation, using additional instruments such as codes of conduct, while ensuring that these principles are well-known, understood and applied by all players who process health-related data and taken into account in the design, deployment and use of the information and communication technologies (ICTs) in that sector.

Appendix to Recommendation CM/Rec(2018)…

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 highlights the importance of developing secured interoperable information systems.

2. Scope

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

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

3. Definitions

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

- The expression “personal data” refers to any information relating to an identified or identifiable individual (“data subject”).

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

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

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

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

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

- The expression “controller” means the natural or legal person, public authority, service, agency or any other body which, alone or jointly with others, has the decision-making power with respect to data processing.

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

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

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

- The expression “health professionals” covers all professionals recognised as such by law practising in the health, medical welfare or social welfare sector, bound by a confidentiality obligation and involved in providing health care.

- The expression "external data hosting" denotes the use of third party data 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 transparent, lawful and fair manner.

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

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

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

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

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

g. The rights of the person whose data are processed must be respected, particularly the rights of access to the data, information, rectification, objection, and deletion as provided for in principles 11 and 12 of this Recommendation.

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

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

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

5. Legitimate basis of health-related data processing

Processing is only lawful if and to the extent that the controller can rely on at least one of the legitimate basis described in the following paragraphs:

5.1 Without prejudice to the situations covered by the subsequent paragraphs, health-related data may only be processed where appropriate safeguards are enshrined in law and the processing is necessary for:

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

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

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

d. reasons relating to the obligations of the controllers and to the exercise of their rights or those of the data subject regarding employment and social protection, in accordance with law or any collective agreement complying with the said law;

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

f. processing for archiving purposes in the public interest, for scientific or historical research purposes or statistical purposes subject to the conditions defined by law in order to guarantee protection of the data subject's fundamental rights and legitimate interests (see in particular the conditions applicable to the processing of health-related data for scientific research under Chapter V);

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

h. reasons of substantial public interest, on the basis of law, which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

5.2 Health-related data may be processed if the data subject has given her or his consent, except in cases where law provides that a ban on health-related data processing cannot be lifted solely by the data subject's consent. Where consent of the data subject to the processing of health-related data is required, in accordance with law, it should be free, specific, informed and explicit. Consent can be expressed by electronic means. The data subject shall be informed of her or his right to withdraw consent at any time and be notified that such withdrawal shall not affect the lawfulness of the processing carried out on the basis of her or his consent before withdrawal. It shall be as easy to withdraw as to give consent.

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

5.4 Health-related data manifestly made public by the data subject can be processed.

5.5 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 by law with a view to safeguarding respect for rights and fundamental freedoms.

6. Data concerning unborn children

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

7. Health-related genetic data

7.1 Genetic data should only be collected subject to appropriate safeguards and where it is either prescribed by law or on the basis of the consent expressed by the data subject in accordance with the provisions of paragraph 5.2, except where consent is excluded by law as legal basis for the processing of genetic data.

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

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

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

7.5 The data subject is entitled to know any information collected about her or his health. Furthermore, the data subject may have her or his own reasons for not wishing to know about certain health aspects and anyone should be informed, prior to any analysis, of the possibility of not being informed of the results, including of unexpected findings. Her or his wish not to know may, in exceptional circumstances, have to be restricted as foreseen by law, notably in the data subject's own interest or in light of the doctors' duty to provide care.

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

8.1 Where health-related data are shared by different professionals for purposes of providing and administering health care of an individual, the data subject shall be informed beforehand, except where this proves to be impossible due to an emergency or in accordance with principle 11.4. Where the sharing is based on the consent of the data subject, such consent can be withdrawn at any time in accordance with principle 5.2. Where the sharing is authorised by law, the data subject can object to the sharing of her or his health-related data.

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

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

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

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

9. Communication of health-related data for other purposes than providing and administering health care

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

9.2 Insurance companies and employers cannot, in principle, be regarded as recipients authorised to have access to the health-related data of patients unless law provides for this with appropriate safeguards and if the data subject has consented to it in accordance with the conditions of principle 5.2.

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

10. Storage of health-related data

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

Chapter III. The rights of the data subject

11. Transparency of processing

11.1 The data subject must be informed by the controller of the processing of her or his 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 the relevant legal basis for it,
- the length of preservation of the data,
- the recipients or categories of recipients of the data, and planned data transfers to a third country, or an international organisation,
- the possibility, if applicable, of objecting to the processing of her or his data, in the conditions prescribed in principle 12.2,
- the conditions and the means made available to her or him for exercising via the controller her or his rights of access, of rectification and to erasure of her or his health-related data.

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

- that her or his data may subsequently be processed for a compatible purpose, in accordance with appropriate safeguards provided for by law and in the conditions prescribed in paragraph 4.1.b,
- the specific techniques used to process her or his health-related data,
- the possibility of lodging a complaint with a supervisory authority,

- the existence of automated decisions, including profiling which is only permissible where prescribed by law and subject to appropriate safeguards.

11.2 This information should be provided prior to data collection or at the first communication.

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

11.4 A derogation to the right of information is admissible where the data subject already has the necessary information. Moreover, where the personal data are not collected from the data subject, the controller should not be required to provide such information where the processing is expressly prescribed by law or this proves to be impossible or involves disproportionate efforts from the controller, in particular for processing for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes.

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

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

12. Access to data, rectification, erasure, objection to the processing and data portability

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

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

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

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

12.4 The data subject shall have the right not to be subject to a decision significantly affecting her or him based solely on an automated processing, including profiling (see in particular Recommendation (2010)13 of the Committee of Ministers on the protection of individuals with regard to automatic processing of personal data in the context of

profiling), of her or his health-related data. This prohibition can only be derogated to where the law provides that such a processing can be based on the consent of the data subject or that the processing is necessary for reasons of substantial public interest, such a law should be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific safeguards to protect the fundamental rights and freedoms of the data subject.

12.5 Data subjects should be able to obtain from the controller, subject to conditions prescribed by law, where the processing is performed by automatic means, the transmission - in a structured, interoperable and machine-readable format - of their personal data with a view to transmitting them to another controller (data portability). The data subject should also be able to require from the controller that he or she transmits directly the data to another controller.

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

12.7 The right to be informed and the other rights of the data subject 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.

Chapter IV. Security and interoperability

13. Security

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

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

13.3 System availability – i.e. the proper functioning of the system – should be ensured by measures enabling the data to be made accessible in a secure way and with due regard for the level of permission of authorised persons.

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

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

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

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

14. Interoperability

14.1 Interoperability, which is the ability of different information systems to communicate and exchange data, may help address important needs in the health sector. It may provide technical means to facilitate the updating of information or to avoid storage of identical data in multiple databases and contribute to data portability.

14.2 It is however necessary that interoperability be carried out in full compliance with the principles provided for by this Recommendation, in particular the principles of lawfulness, necessity and proportionality and that data protection safeguards be put in place when using interoperable systems.

14.3 Reference frameworks, offering a technical frame, facilitating interoperability based on international norms, should ensure that a high level of security is guaranteed while providing for such interoperability. The monitoring of the implementation of such reference frameworks can be done through certification schemes.

Chapter V. Scientific research

15. Scientific research

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

15.2 The need to process health-related data for the purposes of scientific research should be evaluated in light of the aim pursued and the risks to the data subject and, as concerns the processing of genetic data, in light of the risk to the biological family.

15.3 Health-related data should only be processed in a research project if the data subject has consented to it in accordance with the provisions of principles 5.2. As an exception, the law may provide for the processing of health-related data for scientific research. Such a law should be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific safeguards to protect the fundamental rights and freedoms of the data subject. These safeguards should especially include the obligation to put in place technical and organisational measures to ensure the respect for the principle of data minimisation.

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

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

15.5 The controller should not be obliged to provide the information if the conditions laid down in principle 11.4 are fulfilled. Moreover, law may provide for derogations from the controller's obligation to inform the data subject if the health-related data have not been obtained from the data subject and the obligation to inform the data subject is likely to render impossible or seriously impair the achievement of the specific research purposes. In such cases the controller should take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available.

15.6 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 express consent for certain areas of research or certain parts of research projects, to the extent allowed by the intended purpose, with due regard for recognised ethical standards.

15.7 The conditions in which health-related data are processed for scientific research must be assessed, where necessary, by the competent body designated by law (ethics committee).

15.8 Healthcare professionals who are entitled to carry out their own medical research and scientists in other disciplines should be able to use the health-related data which they hold as long as the data subject has been informed of this possibility beforehand in compliance with paragraph 15.4 and subject to complementary safeguards determined by law such as requiring explicit consent or the assessment of the competent body designated by law.

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

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

15.11 Personal data used for scientific research should not be published in a form which enables the data subject to be identified, except:

a. where the data subject has consented to it, or

b. where law permits such publication under the condition that this is indispensable for the presentation of research findings on contemporary events and only to the extent that the interest in publishing the data overrides the interests and fundamental rights and freedoms of the data subject.

Chapter VI. Mobile applications

16. Mobile applications

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

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

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

16.4 The external hosting 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.

Chapter VII. Transborder flows of health-related data

17. Protecting health-related data flows

17.1 Health-related data processing under all its varied and diverse forms (mobile applications, sharing, global cloud environment, etc.) implies an increase in the transborder nature of such processing.

17.2 Transborder data flows may only take place where an appropriate level of data protection is secured in accordance with the safeguards provided for in Convention 108, or on the basis of the following derogatory regime aimed at allowing a transfer to a recipient which does not ensure such an appropriate level of protection:

a. the data subject has given her or his consent to the transfer, after being informed of risks arising in the absence of appropriate safeguards; or
b. the specific interests of the data subject require it in the particular case; or
c. prevailing legitimate interests, in particular important public interests, are provided for by law and such transfer constitutes a necessary and proportionate measure in a democratic society.