COMMITTEE OF MINISTERS
COMITÉ DES MINISTRES

1949.2019

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

MINISTERS' DEPUTIES Recommendations **CM/Rec(2019)2** 27 March 2019

Recommendation CM/Rec(2019)2 of the Committee of Ministers to member States on the protection of health-related data

(Adopted by the Committee of Ministers on 27 March 2019 at the 1342nd meeting of the Ministers' Deputies)

The Committee of Ministers, under the terms of Article 15.*b* of the Statute of the Council of Europe,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Aware of the growing use of new technologies in processing health-related data;

Having regard to the provisions of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[1] 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), and convinced of the desirability of facilitating the application of those principles to the processing of health-related data;

Observing that 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 No. R (97) 5 of the Committee of Ministers to member States on the protection of medical data;

Realising that 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;

Considering that the benefits of this increasing digitisation of data can be found in numerous areas, such as the enhancement of public health policies, medical treatment or patient care, and that 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 the effective protection of every individual;

Noting 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;

Noting furthermore that geographical mobility and the development of mobile health applications, medical devices and connected objects are also contributing to new uses and to the production of a rapidly growing volume of health-related data processed by more diverse stakeholders;

[1]. The Protocol amending Convention 108 (CETS No. 223) was opened for signature on 10 October 2018 and the revised convention has yet to enter into force.

Observing that this assessment shared by the member States has prompted the replacement of Recommendation No. R(97)5 of the Committee of Ministers to member States on the protection of medical data, and the use of the more general term “health-related data” in this new Recommendation, 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;

Considering that health-related data belong to a special category which, under Article 6 of Convention 108, enjoys a higher level of protection due notably to the risk of discrimination which may occur with their processing;

Convinced that everyone is entitled to the protection of their health-related data, and that individuals receiving care are entitled, when dealing with a professional operating in the health-care and social welfare sectors, to respect for their privacy and the confidentiality of their information;

Stressing that the processing of health-related data should always aim to serve the data subject or to enhance the quality and efficiency of care, and to enhance health systems where possible, while respecting individuals’ fundamental rights,

Recommends that the governments of member States:

- take steps to ensure that the principles set forth in the appendix to this Recommendation, which replaces the above-mentioned Recommendation No. R(97)5, 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 health-care systems, which will then be responsible for promoting their transmission to the various actors processing health-related data, in particular health-care 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 everyone who processes health-related data and are taken into account in the design, deployment and use of information and communication technologies (ICTs) in that sector.

Appendix to Recommendation CM/Rec(2019)2

Chapter I – General provisions

1. Purpose

The purpose of this Recommendation is to provide member States with guidelines on regulating the processing of health-related data in order to guarantee respect for the rights and fundamental freedoms of every individual, in particular the right to privacy and to protection of personal data as required by Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 5, "European Convention on Human Rights"). It therefore highlights the importance of developing secure, interoperable information systems.

2. Scope

2.1. This Recommendation is applicable to the processing of personal data relating to health in the public and private sectors. It therefore 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 the law to grant wider protection to data subjects.

2.2. 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 terms shall be defined as follows:

- "personal data" refers to any information relating to an identified or identifiable individual ("data subject");

- "data processing" means any operation or set of operations 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;

- "anonymisation" refers to the process applied to personal data so that the data subjects can no longer be identified, either directly or indirectly;

- "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;

- "health-related data" means all personal data concerning the physical or mental health of an individual, including the provision of health-care services, which reveals information about this individual's past, current and future health;

- "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;

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

- "processor" means a natural or legal person, public authority, service, agency or any other body which processes data on behalf of the controller;

- "reference framework" denotes a co-ordinated set of rules and/or state-of-the-art processes, 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;

- “interoperability” denotes the ability to communicate and exchange data across different information systems;

- “mobile devices” means a set of tools accessible in a mobile environment making it possible to communicate and manage health-related data remotely. They may take different forms, such as connected medical objects and devices which can be used for diagnostic, treatment or well-being purposes, among other things;

- “health professionals” means all professionals recognised as such by law practising in the health-care and social welfare sectors, and who are bound by a confidentiality obligation and involved in providing health care;

- “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 – 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, historical research 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.*b,* or on some other legitimate basis, as laid down in the 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 personal data, or its destruction, loss, use, unavailability, inaccessibility, modification or disclosure.

g. The rights of the individual whose data are processed must be respected, particularly the right of access to the data and the rights to 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 foreseen processing of data 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 on 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 bases described in the following paragraphs.

a. 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:

preventive medical purposes and purposes of medical diagnosis, administration of care or treatment, or management of health services by health professionals and those of health-care and social welfare sectors, subject to the conditions provided for by law;

- reasons of public health, such as the 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 provided for by law;

- the purpose of safeguarding the vital interests of the data subject or of another individual where consent cannot be collected;

- 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 it;

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

- processing for archiving purposes in the public interest or for the purposes of scientific or historical research or statistics, 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);

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

- 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.

b. Health-related data may be processed if the data subject has given their 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. The data subject shall be informed of their 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 their consent before withdrawal. It shall be as easy to withdraw consent as it is to give it.

c. 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 their behalf with a health professional subject to conditions defined by law, including the obligation of secrecy.

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

e. 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, such as data resulting from a prenatal diagnosis or from the identification of the genetic characteristics of such children, should benefit from 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.*b*, except where consent is excluded by law as a legal basis for the processing of genetic data. The provisions of Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment are to be taken into consideration where the processing of genetic data occurs in an employment context.

7.2. Genetic data processed with a preventive aim, for diagnosis or for treatment of the data subject or a member of their 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 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. Processing of genetic data can be used for the purpose of identification of individuals in a humanitarian crisis or action where appropriate safeguards are provided for by law.

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 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 CM/Rec(2016)8 of the Committee of Ministers to member States 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 this regard.

7.6. The data subject is entitled to know any information relating to their genetic data, subject to the provisions of principles 11.8 and 12.7. Nevertheless, the data subject may have their own reasons for not wishing to know about certain health aspects and everyone should be aware, prior to any analysis, of the possibility of not being informed of the results, including of unexpected findings. Their 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 to an individual, the data subject shall be informed beforehand, except where this proves impossible due to an emergency or in accordance with principle 11.6. 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.*b*. Where the sharing is authorised by law, the data subject can object to the sharing of their health-related data.

8.2. Professionals working on a particular individual case in the health-care and social welfare sectors 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 monitoring of the individual. The respective health professionals are only able in this case to share or receive data 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 purposes other than providing and administering health care

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

9.2. Insurance companies cannot be regarded as recipients authorised to have access to the health-related data of individuals unless law provides for this with appropriate safeguards and in accordance with principle 5.

9.3. Employers cannot be regarded as recipients authorised to have access to the health-related data of individuals except in the conditions provided for by Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment.

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

10. Storage of health-related data

Health-related 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 or for the purposes of scientific or historical research or statistics and where appropriate measures are in place 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 – Rights of the data subject

11. Transparency of processing

11.1. The controller must inform the data subject of the processing of their health-related data.

11.2. 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 their data, under the conditions prescribed in principle 12.2;
- the conditions and the means made available to the data subject for exercising, via the controller, their rights of access, rectification and erasure of their data.

11.3. Where necessary and with a view to ensuring fair and transparent processing, the information must also include:

- the possibility that their data may subsequently be processed for a compatible purpose, in accordance with appropriate safeguards provided for by law and in accordance with the conditions prescribed in paragraph 4.1.*b*;
- 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.

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

11.5. The information must be intelligible and easily accessible, in clear and plain language and suited to the circumstances to allow the data subject to fully understand the foreseen processing. In particular, where the data subject is physically or legally incapable of receiving the information, it may be given to the person legally representing them. If a legally incapacitated person is capable of understanding, they should also be informed before the data are processed.

11.6. The controller is not required to provide this information where the data subject already has the necessary information. Moreover, where the personal data are not collected directly from the data subject, the controller is not required to inform them where the processing is expressly prescribed by law or this proves to be impossible, for instance where the contact details of the individual have changed and the individual cannot be found or is not reachable, or it involves disproportionate efforts from the controller, in particular for processing for archiving purposes in the public interest and for purposes of scientific or historical research or statistics.

11.7. An individual's wish not to be informed of a diagnosis or prognosis should be complied with, except where this constitutes a serious risk for the health of others.

11.8. The controller is not required to inform the data subject where this is provided for by law and is necessary and proportionate in a democratic society for the reasons specified in Article 9 of Convention 108.

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 them are being processed, and, if so, to obtain – without excessive delay or expense and in an intelligible form – communication of their 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 that underlies data processing where the results of such processing are applied to them, notably in the case of profiling.

12.2. The data subject has the right to erasure of data processed in violation of the provisions of Convention 108. The data subject is entitled to obtain rectification of data concerning them. The data subject furthermore has the right to object on grounds relating to their personal situation to the processing of their 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, some remedy should be available to them.

12.4. The data subject shall have the right not to be subject to a decision significantly affecting them based solely on the automated processing, including profiling,[2] of their health-related data. States should only derogate from this prohibition where the law provides that such processing can be based on the consent of the data subject or that it is necessary for reasons of substantial public interest. The measures provided for in 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. Where the processing is performed by automatic means, the data subject should be able to obtain from the controller, subject to conditions prescribed by law 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 the controller to transmit the data directly to another controller.

12.6. Health professionals must put in place all necessary measures in order to ensure respect for the effective exercise of such rights as part of their professional ethics.

12.7. The rights of the data subject can be subject to restrictions where such restrictions are provided for by law and are necessary and proportionate measures in a democratic society for the reasons specified in Article 9 of Convention 108.

12.8. The law should provide for appropriate safeguards ensuring the respect of the data subject's rights.

Chapter IV – Security and interoperability

13. Security

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

13.2. Data security provisions, provided for by law or other regulations, and contained in reference frameworks, as the case may be, should result in regularly reviewed, state-of-the-art technical and organisational measures so as to protect personal health-related data from any illegal or accidental destruction, any loss or any alteration, 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 – namely, 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 presumes verification of the actions 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 database and the data themselves, ensuring that only authorised persons are able to access the data.

13.5. "Auditability" should lead to a system in which it is possible to trace any access to the information system, modifications made and any action carried out, in order to identify its author.

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

13.7. Professionals who are not directly involved in the individual's health care, but by virtue of their assigned tasks ensure the smooth operation of information systems, may have access, insofar as 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 by law to guarantee the confidentiality and security of the data.

[2]. See notably Recommendation CM/Rec(2010)13 of the Committee of Ministers to member States on the protection of individuals with regard to automatic processing of personal data in the context of profiling.

14. Interoperability

14.1. Interoperability may help address important needs in the health sector and 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 for interoperability to be implemented in full compliance with the principles provided for in this Recommendation, in particular the principles of lawfulness, necessity and proportionality, and for data protection safeguards to be put in place when interoperable systems are used.

14.3. Reference frameworks based on international norms offering a technical structure which facilitates interoperability should guarantee a high level of security while providing for such interoperability. The monitoring of the implementation of such reference frameworks can be carried out 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, 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 scientific research should be evaluated in light of the purposes of the research project, 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, in principle, only be processed in a scientific research project if the data subject has consented to it in accordance with the provisions of principle 5.*b.* However, the law may provide for the processing of health-related data for scientific research without the data subject's consent. The provisions of 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 include, in particular, the obligation to put in place technical and organisational measures to ensure 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 they could make, 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 the rights to refuse to participate in the research and to withdraw at any time.

15.5. The controller should not be obliged to provide the information if the conditions laid down in principle 11.6 are fulfilled. Moreover, and without prejudice to the provisions of Recommendation CM/Rec(2016)6 of the Committee of Ministers to member States on research on biological materials of human origin, the 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, fundamental 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 independent body (for example, an 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; where research purposes do not allow this, 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. These measures must be carried out 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 project, their health-related data processed in the context of that research should be destroyed or anonymised in a manner which does not 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 the law permits such publication on the condition that it 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 devices

16. Mobile devices

16.1 Where the data collected by mobile devices, implanted in the individual or not, may reveal information on the physical or mental state of an individual in connection with their health and well-being or concern any information regarding health-care and social welfare provision, 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 this Recommendation.

16.2 Individuals using such mobile devices which involve the processing of their personal data should enjoy the same rights as those provided for in Chapter III of this Recommendation. They must notably have been provided beforehand with all necessary information on the nature and functioning of the system in order to be able to control its use. To this end, 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 must be determined in advance.

16.3. Any use of mobile devices must be accompanied by specific, customised 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 devices 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

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 regime of derogations aimed at allowing a transfer to a recipient which does not ensure an appropriate level of protection:

a. the data subject has given explicit, specific and free 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 a transfer constitutes a necessary and proportionate measure in a democratic society; or
d. the transfer constitutes a necessary and proportionate measure for freedom of expression in a democratic society.