

COUNCIL OF EUROPE

COMMITTEE OF MINISTERS

RECOMMENDATION No. R (97) 5

OF THE COMMITTEE OF MINISTERS TO MEMBER STATES ON THE PROTECTION OF MEDICAL DATA

*(Adopted by the Committee of Ministers on 13 February 1997
at the 584th 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;

Recalling the general principles on data protection in the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (European Treaty Series, No. 108) and in particular its Article 6 which stipulates that personal data concerning health may not be processed automatically unless domestic law provides appropriate safeguards;

Aware of the increasing use of automatic processing of medical data by information systems, not only for medical care, medical research, hospital management and public health but also outside the health-care sector;

Convinced of the importance of the quality, integrity and availability of medical data for the health of the data subject and his family;

Aware that progress in medical science is dependent to a great extent on the availability of medical data on individuals;

Convinced that it is desirable to regulate the collection and processing of medical data, to safeguard the confidentiality and security of personal data regarding health, and to ensure that they are used subject to the rights and fundamental freedoms of the individual, and in particular the right to privacy;

Aware that progress made in medical science and developments in information technology since 1981 have made it necessary to revise various provisions in Recommendation No. R (81) 1 on regulations for automated medical data banks,

Recommends that the governments of member states:

- take steps to ensure that the principles contained in the appendix to this recommendation are reflected in their law and practice;

- ensure wide circulation of the principles contained in the appendix to this recommendation among persons professionally involved in the collection and processing of medical data;

Decides that this recommendation will replace Recommendation No. R (81) 1 on regulations for automated medical data banks.

Appendix to Recommendation No. R (97) 5

1. Definitions

For the purposes of this recommendation:

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

– the expression “medical data” refers to all personal data concerning the health of an individual. It refers also to data which have a clear and close link with health as well as to genetic data;

– the expression “genetic data” refers to all data, of whatever type, concerning the hereditary characteristics of an individual or concerning the pattern of inheritance of such characteristics within a related group of individuals.

It also refers to all data on the carrying of any genetic information (genes) in an individual or genetic line relating to any aspect of health or disease, whether present as identifiable characteristics or not.

The genetic line is the line constituted by genetic similarities resulting from procreation and shared by two or more individuals.

2. Scope

2.1. This recommendation is applicable to the collection and automatic processing of medical data, unless domestic law, in a specific context outside the health-care sector, provides other appropriate safeguards.

2.2. A member state may extend the principles set out in this recommendation to cover medical data not processed automatically.

3. Respect for privacy

3.1. The respect of rights and fundamental freedoms, and in particular of the right to privacy, shall be guaranteed during the collection and processing of medical data.

3.2. Medical data may only be collected and processed if in accordance with appropriate safeguards which must be provided by domestic law.

In principle, medical data should be collected and processed only by health-care professionals, or by individuals or bodies working on behalf of health-care professionals. Individuals or bodies working on behalf of health-care professionals who collect and process medical data should be subject to the same rules of confidentiality incumbent on health-care professionals, or to comparable rules of confidentiality.

Controllers of files who are not health-care professionals should only collect and process medical data subject either to rules of confidentiality comparable to those incumbent upon a health-care professional or subject to equally effective safeguards provided for by domestic law.

4. Collection and processing of medical data

4.1. Medical data shall be collected and processed fairly and lawfully and only for specified purposes.

4.2. Medical data shall in principle be obtained from the data subject. They may only be obtained from other sources if in accordance with Principles 4, 6 and 7 of this recommendation and if this is necessary to achieve the purpose of the processing or if the data subject is not in a position to provide the data.

4.3. Medical data may be collected and processed:

a. if provided for by law for:

i. public health reasons; or

ii. subject to Principle 4.8, the prevention of a real danger or the suppression of a specific criminal offence; or

iii. another important public interest; or

b. if permitted by law:

i. for preventive medical purposes or for diagnostic or for therapeutic purposes with regard to the data subject or a relative in the genetic line; or

ii. to safeguard the vital interests of the data subject or of a third person; or

iii. for the fulfilment of specific contractual obligations; or

iv. to establish, exercise or defend a legal claim; or

c. if the data subject or his/her legal representative or an authority or any person or body provided for by law has given his/her consent for one or more purposes, and in so far as domestic law does not provide otherwise.

4.4. If medical data have been collected for preventive medical purposes or for diagnostic or therapeutic purposes with regard to the data subject or a relative in the genetic line, they may also be processed for the management of a medical service operating in the interest of the patient, in cases where the management is provided by the health-care professional who collected the data, or where the data are communicated in accordance with principles 7.2 and 7.3.

Unborn children

4.5. Medical data concerning unborn children should be considered as personal data and enjoy a protection comparable to the protection of the medical data of a minor.

4.6. Unless otherwise provided for by domestic law, the holder of parental responsibilities may act as the person legally entitled to act for the unborn child, the latter being a data subject.

Genetic data

4.7. Genetic data collected and processed for preventive treatment, diagnosis or treatment of the data subject or for scientific research should only be used for these purposes or to allow the data subject to take a free and informed decision on these matters.

4.8. Processing of genetic data for the purpose of a judicial procedure or a criminal investigation should be the subject of a specific law offering appropriate safeguards.

The data should only be used to establish whether there is a genetic link in the framework of adducing evidence, to prevent a real danger or to suppress a specific criminal offence. In no case should they be used to determine other characteristics which may be linked genetically.

4.9. For purposes other than those provided for in Principles 4.7 and 4.8, the collection and processing of genetic data should, in principle, only be permitted for health reasons and in particular to avoid any serious prejudice to the health of the data subject or third parties.

However, the collection and processing of genetic data in order to predict illness may be allowed for in cases of overriding interest and subject to appropriate safeguards defined by law.

5. Information of the data subject

5.1. The data subject shall be informed of the following elements:

- a. the existence of a file containing his/her medical data and the type of data collected or to be collected;
- b. the purpose or purposes for which they are or will be processed;
- c. where applicable, the individuals or bodies from whom they are or will be collected;
- d. the persons or bodies to whom and the purposes for which they may be communicated;
- e. the possibility, if any, for the data subject to refuse his consent, to withdraw it and the consequences of such withdrawal;
- f. the identity of the controller and of his/her representative, if any, as well as the conditions under which the rights of access and of rectification may be exercised.

5.2. The data subject should be informed at the latest at the moment of collection. However, when medical data are not collected from the data subject, the latter should be notified of the collection as soon as possible, as well as – in a suitable manner – of the information listed under Principle 5.1, unless this is clearly unreasonable or impracticable, or unless the data subject has already received the information.

5.3. Information for the data subject shall be appropriate and adapted to the circumstances. Information should preferably be given to each data subject individually.

5.4. Before a genetic analysis is carried out, the data subject should be informed about the objectives of the analysis and the possibility of unexpected findings.

Legally incapacitated persons

5.5. If the data subject is a legally incapacitated person, incapable of free decision and domestic law does not permit the data subject to act on his/her own behalf, the information shall be given to the person recognised as legally entitled to act in the interest of the data subject.

If a legally incapacitated person is capable of understanding, he/she should be informed before his/her data are collected or processed.

Derogations

5.6. Derogations from Principles 5.1, 5.2 and 5.3 may be made in the following cases:

- a. information of the data subject may be restricted if the derogation is provided for by law and constitutes a necessary measure in a democratic society:
 - i. to prevent a real danger or to suppress a criminal offence;
 - ii. for public health reasons;
 - iii. to protect the data subject and the rights and freedoms of others;
- b. in medical emergencies, data considered necessary for medical treatment may be collected prior to information.

6. Consent

6.1. Where the data subject is required to give his/her consent, this consent should be free, express and informed.

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

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

If, in accordance with Principle 5.5 above, a legally incapacitated person has been informed of the intention to collect or process his/her medical data, his/her wishes should be taken into account, unless domestic law provides otherwise.

7. Communication

7.1. Medical data shall not be communicated, unless on the conditions set out in this principle and in Principle 12.

7.2. In particular, unless other appropriate safeguards are provided by domestic law, medical data may only be communicated to a person who is subject to the rules of confidentiality incumbent upon a health-care professional, or to comparable rules of confidentiality, and who complies with the provisions of this recommendation.

7.3. Medical data may be communicated if they are relevant and:

- a. if the communication is provided for by law and constitutes a necessary measure in a democratic society for:
 - i. public health reasons; or
 - ii. the prevention of a real danger or the suppression of a specific criminal offence; or
 - iii. another important public interest; or
 - iv. the protection of the rights and freedoms of others; or
- b. if the communication is permitted by law for the purpose of:
 - i. the protection of the data subject or a relative in the genetic line;
 - ii. safeguarding the vital interests of the data subject or a third person; or
 - iii. the fulfilment of specific contractual obligations; or
 - iv. establishing, exercising or defending a legal claim; or
- c. if the data subject or his/her legal representative, or an authority, or any person or body provided for by law has given his/her consent for one or more purposes, and in so far as domestic law does not provide otherwise; or
- d. provided that the data subject or his/her legal representative, or an authority, or any person or body provided for by law has not explicitly objected to any non-mandatory communication, if the data have been collected in a freely chosen preventive, diagnostic or therapeutic context, and if the purpose of the communication, in particular the provision of care to the patient or the management of a medical service operating in the interest of the patient, is not incompatible with the purpose of the processing for which they were collected.

8. Rights of the data subject

Rights of access and of rectification

8.1. Every person shall be enabled to have access to his/her medical data, either directly or through a health-care professional or, if permitted by domestic law, a person appointed by him/her. The information must be accessible in understandable form.

8.2. Access to medical data may be refused, limited or delayed only if the law provides for this and if:

- a. this constitutes a necessary measure in a democratic society in the interests of protecting state security, public safety, or the suppression of criminal offences; or
- b. knowledge of the information is likely to cause serious harm to the data subject's health; or
- c. the information on the data subject also reveals information on third parties or if, with respect to genetic data, this information is likely to cause serious harm to consanguine or uterine kin or to a person who has a direct link with this genetic line; or
- d. the data are used for statistical or for scientific research purposes where there is clearly no risk of an infringement of the privacy of the data subject, notably the possibility of using the data collected in support of decisions or measures regarding any particular individual.

8.3. The data subject may ask for rectification of erroneous data concerning him/her and, in case of refusal, he/she shall be able to appeal.

Unexpected findings

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

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

Subject to sub-paragraph *a*, the person should also be informed if this information is of direct importance to him/her for treatment or prevention.

9. Security

9.1. Appropriate technical and organisational measures shall be taken to protect personal data – processed in accordance with this recommendation – against accidental or illegal destruction, accidental loss, as well as against unauthorised access, alteration, communication or any other form of processing.

Such measures shall ensure an appropriate level of security taking account, on the one hand, of the technical state of the art and, on the other hand, of the sensitive nature of medical data and the evaluation of potential risks.

These measures shall be reviewed periodically.

9.2. In order to ensure in particular the confidentiality, integrity and accuracy of processed data, as well as the protection of patients, appropriate measures should be taken:

- a. to prevent any unauthorised person from having access to installations used for processing personal data (control of the entrance to installations);
- b. to prevent data media from being read, copied, altered or removed by unauthorised persons (control of data media);
- c. to prevent the unauthorised entry of data into the information system, and any unauthorised consultation, modification or deletion of processed personal data (memory control);
- d. to prevent automated data processing systems from being used by unauthorised persons by means of data transmission equipment (control of utilisation);
- e. with a view to, on the one hand, selective access to data and, on the other hand, the security of the medical data, to ensure that the processing as a general rule is so designed as to enable the separation of:
 - identifiers and data relating to the identity of persons;

- administrative data;
 - medical data;
 - social data;
 - genetic data (access control);
- f. to guarantee the possibility of checking and ascertaining to which persons or bodies personal data can be communicated by data transmission equipment (control of communication);
- g. to guarantee that it is possible to check and establish *a posteriori* who has had access to the system and what personal data have been introduced into the information system, when and by whom (control of data introduction);
- h. to prevent the unauthorised reading, copying, alteration or deletion of personal data during the communication of personal data and the transport of data media (control of transport);
- i. to safeguard data by making security copies (availability control).

9.3. Controllers of medical files should, in accordance with domestic law, draw up appropriate internal regulations which respect the related principles in this recommendation.

9.4. Where necessary, controllers of files processing medical data should appoint an independent person responsible for security of information systems and data protection and competent for giving advice on these issues.

10. Conservation

10.1. In general, medical data shall be kept no longer than necessary to achieve the purpose for which they were collected and processed.

10.2. When, in the legitimate interest of public health, medical science, the person in charge of the medical treatment or the controller of the file, in order to enable him/her to defend or exercise a legal claim, or for historical or statistical reasons, it proves necessary to conserve medical data that no longer serve their original purpose, technical arrangements shall be made to ensure their correct conservation and security, taking into account the privacy of the patient.

10.3. On the request of the data subject, his/her medical data should be erased – unless they have been made anonymous or there are overriding and legitimate interests, in particular those stated in Principle 10.2 not to do so, or there is an obligation to keep the data on record.

11. Transborder flows

11.1. The principles of this recommendation are applicable to the transborder flow of medical data.

11.2. The transborder flow of medical data to a state which has ratified the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, and which disposes of legislation which provides at least equivalent protection of medical data, should not be subjected to special conditions concerning the protection of privacy.

11.3. Where the protection of medical data can be considered to be in line with the principle of equivalent protection laid down in the convention, no restriction should be placed on the transborder flow of medical data to a state which has not ratified the convention but which has legal provisions which ensure protection in accordance with the principles of that convention and this recommendation.

11.4. Unless otherwise provided for by domestic law, the transborder flow of medical data to a state which does not ensure protection in accordance with the convention and with this recommendation, should not as a rule occur unless:

- a. necessary measures, including those of a contractual nature, to respect the principles of the convention and this recommendation, have been taken, and the data subject has the possibility to object to the transfer; or
- b. the data subject has given his consent.

11.5. Unless in the case of emergency or of a transfer to which the data subject has given his informed consent, appropriate measures should be taken to ensure the protection of medical data transferred from one country to another, and in particular:

- a. the person responsible for the transfer should indicate to the addressee the specified and legitimate purposes for which the data have been originally collected, as well as the persons or bodies to whom they may be communicated;
- b. unless otherwise provided for by domestic law, the addressee should undertake, in respect of the person responsible for the transfer, to honour the specified and legitimate purposes which he/she has accepted, and not to communicate the data to persons or bodies other than those indicated by the person responsible for the transfer.

12. Scientific research

12.1. Whenever possible, medical data used for scientific research purposes should be anonymous. Professional and scientific organisations as well as public authorities should promote the development of techniques and procedures securing anonymity.

12.2. However, if such anonymisation would make a scientific research project impossible, and the project is to be carried out for legitimate purposes, it could be carried out with personal data on condition that:

- a. the data subject has given his/her informed consent for one or more research purposes; or
- b. when the data subject is a legally incapacitated person incapable of free decision, and domestic law does not permit the data subject to act on his/her own behalf, his/her legal representative or an authority, or any person or body provided for by law, has given his/her consent in the framework of a research project related to the medical condition or illness of the data subject; or
- c. disclosure of data for the purpose of a defined scientific research project concerning an important public interest has been authorised by the body or bodies designated by domestic law, but only if:
 - i. the data subject has not expressly opposed disclosure; and
 - ii. despite reasonable efforts, it would be impracticable to contact the data subject to seek his consent; and
 - iii. the interests of the research project justify the authorisation; or
- d. the scientific research is provided for by law and constitutes a necessary measure for public health reasons.

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

12.4. As regards any scientific research based on personal data, the incidental problems, including those of an ethical and scientific nature, raised by respect of the provisions of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data should also be examined in the light of other relevant instruments.

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