RECOMMENDATION No. R (81) 1

OF THE COMMITTEE OF MINISTERS TO MEMBER STATES
ON REGULATIONS FOR AUTOMATED MEDICAL DATA BANKS

(Adopted by the Committee of Ministers on 23 January 1981,
at the 328th 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 increasing use of computers for medical care, medi­
cal research, hospital management and public health records;

Convinced that it is desirable to ensure the confidentiality, security
and ethical use of personal information contained in those records;

Recalling the general principles on data protection in the private
and public sectors as set out in its Resolutions (73) 22 and (74) 29 and
the guarantees on the protection of health data of a personal nature
provided by the Convention for the Protection of Individuals with regard
to Automatic Processing of Personal Data;

Observing also that in several member states, guarantees are pro­
vided with the same purpose under existing or draft legislation on data
protection and on medical and professional secrecy;

Considering that it is desirable to provide the persons responsible
for medical data banks with further guidance as to the best way in
which these principles can be implemented with regard to their specific
type of computerised records,

Recommends the governments of member states:

a. to take steps in order to ensure that every automated medical
data bank set up in their territory will be subject to regulations which
reflect the principles laid down in the appendix to this recommendation;
b. to bring this recommendation to the notice of all services, authorities and institutions, both public and private, which operate automated data banks;

c. to promote awareness and information about the protection of medical data among members of the medical profession and data processing specialists and encourage close co-operation in the matter between these two professional groups;

Instructs the Secretary General of the Council of Europe to bring the contents of this recommendation to the notice of the Governments of Australia, Canada, Finland, Japan, the United States of America and Yugoslavia, as well as the Director General of the World Health Organisation.

Appendix to Recommendation No. R (81) 1

Principles applying to automated medical data banks

1. Scope and purpose of the regulations

1.1. The following principles apply to automated data banks set up for purposes of medical care, public health, management of medical or public health services or medical research, in which are stored medical data and, as the case may be, related social or administrative data pertaining to identified or identifiable individuals (automated medical data banks).

1.2. Every automated medical data bank should be subject to its own specific regulations, in conformity with the laws of the state in whose territory it is established.

The regulations of medical data banks used for purposes of public health, management of medical and health services, or for the advancement of medical science should have due regard to the pre-eminence of individual rights and freedoms.

1.3. The regulations should be sufficiently specific to provide ready answers to those questions likely to arise in the operation of the particular medical data bank.

1.4. Where a medical data bank combines several sets of medical records or sub-systems of medical data, each of these elements may require separate supplementary regulations relating to its special features.

1.5. The requirements and obligations following from this recommendation are to be taken duly into account not only with regard to medical data banks which are operational, but also those which are in the development phase.

2. Public notice of automated medical data banks

2.1. Plans for the establishment of automated medical data banks as well as plans for the fundamental modification of existing banks should be brought to the notice of the public in advance.

2.2. When an automated medical data bank becomes operational, a public notice thereof should be given, relating at the very least to the following features:

   a. the name of the medical data bank;

   b. reference to the instrument pursuant to which the medical data bank has been established;

   c. a summary of the data bank’s regulations and an indication of how the complete regulations can be obtained or consulted.

3. Minimum contents of the data bank’s regulations

3.1. The data bank’s regulations should at least contain provisions on:

   a. its specific purpose(s);

   b. the categories of information recorded;

   c. the body or person for whom the data bank is operated and who is competent to decide which categories of data should be processed;

   d. the person(s) in charge of its day-to-day running;

   e. the categories of persons who are entitled to cause data to be placed in storage, modified and erased (“originators of the data”);

   f. the person or body:

      — to whom certain decisions must be submitted for approval;

      — who supervises the use of the data bank;

      — to whom appeal may be made in the event of dispute;

   g. the categories of persons who have access to the data bank in the course of their work and the categories of data to which they are entitled to have access;
8 RECOMMENDATION No. R (81) 1

8. the disclosure of information to third parties;

i. the disclosure of information to the individuals concerned ("data subjects");

j. the long-term conservation of data;

k. the procedure concerning requests for use of data for purpose other than those for which they have been collected;

l. the security of data and installations;

m. whether and on which conditions linking with other data banks is permitted.

4. Recording of data

4.1. The person or body responsible for establishing and/or managing a medical data bank should ensure that:

a. data are collected by lawful and fair means;

b. no data are collected other than those which are relevant and appropriate to the declared purpose(s);

c. so far as is practicable the accuracy of the data is verified; and

d. the contents of the record are kept up to data as appropriate.

4.2. In order to ensure on the one hand selective access to the information in conformity with paragraph 5.1 and on the other hand the security of the data, the records must as a general rule be so designed as to enable the separation of:

a. identifiers and data relating to the identity of persons;

b. administrative data;

c. medical data;

d. social data.

A distinction between objective and subjective data is to be made with regard to the data mentioned under c and d above.

Where, however, it is unnecessary or impossible to achieve such separation, other measures must be taken in order to protect the privacy of individuals and confidentiality of the information.

4.3. A person from whom medical information is collected should be informed of its intended use(s).

5. Access to and use of information

5.1. As a general rule, access to the information may be given only to medical staff and, as far as national law or practice permits, to other health care staff, each person having access to those data which he needs for his specific duties.

5.2. When a person mentioned in the previous paragraph ceases to exercise his functions, he may no longer store, modify, erase or gain access to the data, save by special agreement with the person or body mentioned in paragraph 3.1.f.

5.3. A person referred to in paragraph 5.1 who has access to data in the course of his work may not use such data for a purpose different from that for which he originally had access to those data, unless:

a. he puts the information in such a form that the data subject cannot be identified, or

b. such different use has been authorised by the person or body referred to in paragraph 3.1.f., or

c. such different use is imposed by a provision of law,

It being understood that national law or practice may impose an additional obligation to obtain the consent of the data subject (or, should he be deceased, of his family) or his physician.

5.4. Without the data subject's express and informed consent, the existence and content of his medical record may not be communicated to persons or bodies outside the fields of medical care, public health or medical research, unless such a communication is permitted by the rules on medical professional secrecy.

5.5. Linking or bringing together information on the same individual contained in different medical data banks is permitted for purposes of medical care, public health or medical research, provided it is in accordance with the specific regulations.

6. The data subject and his medical record

6.1. Measures should be taken to enable every person to know of the existence and content of the information about him held in a medical data bank.

This information shall, if the national law so provides, be communicated to the data subject through the intermediary of his physician.
No exception to this principle shall be allowed unless it is prescribed by law or regulation and concerns:

a. data banks which are used only for statistics or scientific research purposes and when there is obviously no risk of an infringement of the privacy of the data subject;

b. information the knowledge of which might cause serious harm to the data subject.

6.2. The data subject may ask for amendment of erroneous data concerning him and, in case of refusal, he may appeal to the person or body referred to in paragraph 3.1.f.

When the information is amended, it may nevertheless be provided that a record will be kept of the erroneous data so far as knowledge of the error may be relevant to further medical treatment or useful for research purposes.

7. Long-term conservation of data

7.1. As a general rule, data relatable to an individual should be kept on record only during a period reasonably useful for reaching their main purpose(s).

7.2. Where, in the interest of public health, medical science, or for historical or statistical purposes, it proves desirable to conserve medical data that have no longer any immediate use, technical provision is to be made for their correct conservation and safekeeping.

8. Professional obligations

In addition to the members of the health care staff, the data processing personnel and any other persons participating in the design, operation, use or maintenance of a medical data bank, must respect the confidential nature of the information and ensure the correct use of the medical data bank.

9. Extended protection

None of the principles in this appendix shall be interpreted as limiting the possibility for a member state to introduce legal provisions granting a wider measure of protection to the persons to whom medical data refer.

EXPLANATORY MEMORANDUM

I. Introduction

1. The use of computers in medicine serves the interests of the individual and of the community.

In the first place, computers contribute towards better medical care by automating techniques, reducing the burden on the doctor's memory and facilitating the establishment of medical records. Medical computer systems are an answer to the increasing demand, caused by specialisation and teamwork, for quick and selective access to information on the patient and his treatment, thus ensuring the continuity of medical care.

2. Medical data processing also brings a major improvement to hospital management and in this way it can help to reduce the cost of health care. Computers are used for recording the admission, transfer and release of patients, keeping track of diagnostic and therapeutic activities, medication, laboratory analyses, accounting, invoicing, etc.

Lastly, medical data processing represents an indispensable instrument for medical research and for a policy of early and systematic diagnosis and prevention of certain diseases.

3. Accordingly, the data concerning an individual's health appear in many files which can be recorded on a computer. The holders of these files vary: the attending physician, the hospital doctor, the school doctor, the works doctor, the medical consultant of an insurance company, hospital administrator, social security offices, etc.

Usually the recording of medical data occurs in the context of the doctor-patient relationship. It takes the form of a medical record which will help to establish the diagnosis, and facilitate the supervision and care of the patient. The information is obtained with the patient's consent by the doctor or a member of the medical team who is required to observe confidentiality under the ethical rules of his profession.
Health records may also be established outside the context of the doctor-patient relationship and may include data concerning perfectly healthy persons. The recording of information is sometimes imposed by a third party, perhaps even without the explicit consent of the person concerned.

4. The quality and integrity of information is extremely important in matters of health. At a time of increasing personal mobility, the exchange of accurate and relevant information is necessary for the individual’s safety. Furthermore, the development of medical science takes place thanks to a transfrontier flow of medical data and the setting up of specialised information systems across considerable geographical distances (such as the Eurotransplant organisation for the transplantation of human organs).

5. The needs which medical data processing systems have to satisfy are often contradictory. Indeed, information must be made rapidly available to duly authorised users whilst remaining inaccessible to others. The obligation to respect the patient’s privacy places certain restrictions on the recording and dissemination of medical data, whereas the right of each individual to health implies that everyone should benefit from the progress made by medical science thanks to extensive use of medical data.

6. Certain of the contents of medical files may harm the patient if used outside the doctor-patient relationship. Medical data comes within the individual’s most intimate sphere. Unauthorised disclosure of personal medical particulars may therefore lead to various forms of discrimination and even to the violation of fundamental rights.

7. Apprehension about abuse of medical information is not due to computer technology as such, for it is generally acknowledged that the use of computers makes it possible to improve considerably the reliability and security of medical data. It is rather a consequence of the awareness that the high technical quality of automated medical records makes it possible to use them for a great variety of purposes.

8. Furthermore, access to medical files is not restricted to doctors alone or to members of the health care staff who are bound to observe medical secrecy. Medical data processing requires the co-operation of numerous persons in other professions outside the medical field, not all of whom are bound by rules of professional secrecy. The use of computers may imply a shift of responsibility between the medical profession and other professions, so that the possibility of an indiscretion is a real danger.

9. Moreover, the emergence of automated data banks has given rise in most countries to a reform of the law according to which individuals will be entitled to know what information is stored about them in computers. The application of this rule in the medical field may cause certain difficulties on account of medical ethics. It should therefore be subject to special safeguards and, as the case may be, restrictions in the interest of the data subjects.

10. In view of these problems, it is highly desirable to make the operation of every automated medical bank subject to a specific set of regulations. The general purpose of these regulations should be to guarantee that medical data are used not only so as to ensure optimum medical care and services but also in such a way that the data subject’s dignity and physical and mental integrity are fully respected.

11. Although such regulations will be adopted by the person or body in charge of each data bank (hospital management, faculty of medicine, etc.), it is desirable that they should follow a common pattern and conform to general principles of data protection.

This follows, inter alia, from the fact that in most countries data protection is, or will be, the subject of legislation. Some laws recently adopted in this field provide that every automated data bank, or at least those data banks which store sensitive information, should have its own regulations.

Consequently, it is up to public authorities to give general guidelines for the drawing up of medical data bank regulations.

12. Furthermore, it appears advisable that the framework for the drafting of these regulations should be European in scale. There are two reasons for this.

First, such a European framework will be the most suitable having regard to the international mobility of people and international exchanges in the field of medicine.

Secondly, national data protection legislation — including therefore protection of medical data — is being harmonised at the European level, on the basis of two resolutions of the Committee of Ministers of the Council of Europe, one of which, adopted in 1973, has laid down data protection principles for the private sector, while the other, adopted a year later, has given similar principles for the public sector.¹ Moreover,

---

¹ Resolution (73) 22 on the protection of the privacy of individuals vis-a-vis electronic data banks in the private sector; Resolution (74) 29 on the protection of the privacy of individuals vis-a-vis electronic data banks in the public sector.
In September 1980, the Committee of Ministers adopted a convention for data protection,\(^1\) which was opened to signature on 28 January 1981. Article 6 of this convention calls for special safeguards for sensitive personal data, including specifically information relating to health.

II. The action taken by the Council of Europe

13. The Council of Europe took up the study of the problem outlined above in February 1976, when the Committee of Ministers established a committee of experts whose task it was \textit{inter alia} "... to carry out a study on data bank regulations, particularly with regard to medical data banks".

14. At its first meeting (29 November — 1 December 1976), the committee of experts on data protection instructed a working party to draw up a draft recommendation. The working party was composed of legal, medical and computer experts from the following countries: France, Norway, Switzerland, Turkey and the United Kingdom.\(^2\) It held four meetings in 1977 and 1978 chaired successively by Mr G. Sandiford and Mr R.A. Harrington (United Kingdom) and assisted by a consultant, Mrs M. Revillard (legal expert at the Centre de recherches, d'information documentation notariales (CRIDON), Lyons).

15. The working party started by examining the special problems raised by the computerisation of medical records relating to individuals. Next, it considered how the general data protection principles contained in Resolutions (73) 22 and (74) 29 should be interpreted and applied in the case of medical data banks.

16. The working party identified a number of data processing problems which are peculiar to medicine, such as, for example:

- the structuring of computerised medical records so that they can be put to various uses;
- the need to keep medical data for periods which are generally very long;
- the problem of the applicability in the medical field of the general rule that it must be possible for the individual to be notified of computerised data concerning him.

17. The working party realised that several of these problems also arose outside the field of data processing. Data processing had, however, intensified the need for a solution.

At the working party's request, the Secretariat collected from members of the plenary committee information on the current legal situation and recent trends in this field in member states.

18. The text which the working party prepared and which was approved, with some modifications by the committee of experts on data protection at its 3rd meeting (16—19 October 1978) took account both of the various trends which have emerged and of the need for progressive harmonisation of member states' legislation. It attempted to strike a fair balance between the rights and interests of individuals on whom medical data are recorded and the public interest.

19. After the European Public Health Committee (CDSP) had adopted at its 7th meeting (16—19 June 1980) an opinion on this text, it was approved, with further amendments, by the European Committee on Legal Co-operation (CDCJ) at its 34th meeting (24—28 November 1980).

20. The recommendation was adopted by the Committee of Ministers, sitting at Deputy level, at its 328th meeting.

III. Detailed comments

Scope and purpose of the regulations

21. The recommendation concerns medical data contained in medical records established in the context of the doctor-patient relationship or in health records established for other purposes.

The term "medical data" includes information concerning the past, present and future, physical or mental health of an individual, as well as related social or administrative information. The latter type of information may relate to a person's address, profession, family circumstances, psychological factors, etc. The information may refer to a data subject who is sick, healthy or deceased. The recommendation is concerned only with such data as can be attributed to identified or identifiable individuals, not with anonymous or aggregate information.

22. In so far as the removal of substances of human origin, or the grafting and the transplantation of tissues or organs have led to the constitution of a medical record, the problem of the protection of the anonymity between the donor and the donee will be covered by this rec-

---

1. Convention for the Protection of Individuals with regard to Automatic Data Processing of Personal Data.
2. Experts from Austria, Ireland and Sweden also attended some of the meetings.
ommendation, since it extends to an individual's past health. Such protection of anonymity between donor and recipient is provided for in general terms in Resolution (78) 29 of the Committee of Ministers of the Council of Europe on harmonisation of legislations of member states relating to removal, grafting and transplantation of human substances.

23. Medical data may appear together with other information in non-medical records, for example insurance or employment records. Such data banks are not covered by the recommendation. However, it is clear that such records may raise important problems in regard to individual freedoms. It should be noted that Article 6 of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data stipulates that personal data concerning health may not be processed automatically unless domestic law provides appropriate safeguards. Under that convention, therefore, it is for contracting states to provide appropriate safeguards for the protection of individuals in cases where data relating to health are processed in data banks not covered by this recommendation.

It is of course highly desirable, in so far as possible, for medical information to be recorded in special data banks and not integrated with general data banks.

24. Automated data banks generally offer better safeguards for the protection, confidentiality and integrity of data than manual systems. However, computerised systems raise specific problems because of the co-operation necessary between members of the medical profession and data processing experts, and because they permit a wider range of uses.

One should not, however, exclude the possibility that the effort expended on this recommendation, which is restricted to computerised systems, may also bear fruit in the sphere of non-computerised medical records.

25. Unlike Resolutions (73) 22 and (74) 29, which provided for two separate series of principles applying to the public and the private sectors, this recommendation applies to medical data banks in both sectors, since they must meet the same requirements and since there is a frequent transfer of data between the two sectors.

26. Further, it is to be observed that the recommendation is designed to allow for the use of medical data for research purposes. In this respect it should be noted that, at the time of publication of this explanatory memorandum, more detailed recommendations for the protection of personal information used for research purposes were being examined by the Council of Europe's committee of experts on data protection.

Of course, the recommendation does not apply to collections of medical statistics which cannot in any way be related to identified or identifiable persons.

Public notice of automated medical data banks

27. In some member states, no automated medical data bank may be established unless the authorities and the public at large have been notified of the fact. It is desirable that, in countries where there is as yet no legal obligation to make a declaration or give public notice of the existence of a medical data bank, those responsible for medical data banks should give such notice in an appropriate form (e.g. by a notice in the press).

28. Publicity of this kind is first and foremost aimed at guaranteeing protection of the individual's rights and freedoms in matters of health. It would also help to make the public aware of the usefulness of computerised medical data systems and, furthermore, may encourage the public to support the introduction of such systems.

29. It is important to note in this connection that the recommendation applies not only to existing operational data banks, but also to those which are in the process of development (project, transition from manual to computerised system, trial installation, etc.). Timely notice of a project for the establishment of a new medical data system will allow interested circles to make their views known before substantial funds have been spent and thereby prevent their being faced with a fait accompli.

Minimum contents of the data bank's regulations

30. Access to the information in a medical data bank must be carefully controlled. This must not result in the medical data bank becoming shrouded in mystery; on the contrary, its regulations must contain such elements as to enable outsiders to obtain an accurate idea of its purpose, the categories of information recorded, its way of operation, etc.

31. For this reason, it must be quite clear from the regulations of the data bank who is the person or body on whose behalf the data bank is operated, who is its manager, who can store information in it, which body exercises supervision over it, to whom requests for information...
and possibly complaints can be addressed, what is the exact nature and purpose of the data recorded, who are the users, etc.

32. While mention may be made of the fact that security measures exist, no precise details must of course be given, in the interests of security itself.

Mention will also be made of the method of erasing obsolete data, the storing of data which no longer serve any immediate purpose and the procedure governing the use of data for purposes other than those for which they were collected.

The preservation of medical records may be required for much longer periods — even going beyond the lifetime of the data subject — than is the case with other kinds of personal records. This is an additional reason why there must be sound data security methods.

Recording of data

33. The data recorded must be accurate and the content of records kept up to date. As regards accuracy, it is obvious that in medicine, errors or inaccuracies may well cause serious damage. However, the consequences of error (e.g. regarding a blood group) can be neutralised if the information provided by the computer is verified with other clinical data submitted for the doctor's assessment. Cross-checking procedures should be used in order to eliminate errors made within the computer system. It is pointed out that detection of an error does not always necessitate a correction (see in this connection paragraph 6.2 of the recommendation).

The requirement that medical data should be up to date derives from the fact that the medical record is intended to guarantee continuity of treatment.

34. Information must be obtained by lawful and fair methods. The present methods of obtaining information from patients are regarded as being generally satisfactory because the patient normally knows what he is being asked for and why. However, there always remains a risk of abuse, having regard to the fact that a patient may be in a state of dependence vis-à-vis the doctor or medical establishment.

35. One of the distinct advantages of computerised records over manual records is that they permit the separation of different types of information (name of the person concerned, administrative, medical or social data, etc.) and that by various technical methods access by the various categories of personnel (medical and paramedical staff, researchers, hospital administrators, etc.) can be restricted, each having access only to such parts of the file as he needs for his specific duties.

Furthermore, objective medical and social data (temperature, blood group, treatment prescribed, social background, profession, etc.) must be kept separate from subjective data (probable diagnosis, likely development of the disease, behaviour, aptitudes, etc.). The words “As a general rule” indicate that the separation of identifying information and other data is not mandatory in all cases. It would be meaningless in the case of a medical data bank which is accessible only to a small number of physicians who all know the identity and illness of the patients.

36. It should also be observed that international harmonisation of forms used to collect information will further the correct entry of data.

37. The words “intended uses” in paragraph 4.3 refer to the general use of medical data (research, hospital records, etc.).

Access to and use of information

38. As the patient is the source of the information, his consent is the basis for the use of information and the conservation of his file by the doctor or the hospital administration.

39. In the interests of the care of patients, the recommendation allows states to grant access to a patient's medical record to members of the medical profession who, because of their functions, are required to observe professional secrecy. A reference to national law and practice is made with regard to access to information by other health care staff (nurses, physiotherapists, etc.), since the definition of that category of personnel and their legal status differs from one country to another, and sometimes even within one country (e.g. in the case of federal states).

40. Since the originator of the data is not the owner of the record, a change in his status or that of any other person having right of access will terminate the possibility for such persons to have access to the data or to record, alter or erase data, without special authorisation.

41. With regard to the use of medical data for purposes other than those originally envisaged, the recommendation draws a clear distinction between persons who have access to the data in the exercise of their functions, and others.
The former, consisting mainly of the medical and health care staff (see paragraph 5.1), may use the information for other purposes (research, teaching, scientific publications, statistics, etc.) provided it is either in anonymous form or by special consent of the person or body named to that effect in the data bank regulations. If it is a person that decides on the follow-up to be given to requests for secondary uses of medical information (see paragraph 3.1.f), he should preferably be a physician. Where this function is entrusted to a collegiate body, it is desirable that not only the medical profession but also the representatives of other interests (patients, social security, etc.) are included in the body's membership. Requests for secondary uses should be duly justified.

42. Under the law or ethical practice of some countries the sole person who can authorise secondary uses of medical information which was obtained in a doctor-patient relationship is the treating physician.

43. Paragraph 5.3.c covers the case where other uses of medical information are imposed by provisions of law (compulsory reporting of a contagious disease, injury caused by an animal suspected of rabies, etc.). Some of these measures are taken as a result of directions from international organisations, such as the World Health Organisation.

44. Paragraph 5.4 deals with the communication of data to other persons or bodies.

Since professional secrecy guarantees that the information disclosed to a doctor will remain confidential, no medical record may be circulated outside the doctor-patient relationship, hospital management, public health services or medical research without the consent of the person concerned, unless such a communication is permitted under the medical profession's rules on secrecy. The doctor-patient relationship naturally includes the patient's relationship with the whole medical team. The circulation of information within this team is in fact essential in the interests of the patient himself.

45. The records sometimes include administrative data which are not automatically covered by professional secrecy. But certain data of an administrative nature, such as the presence of a person in the hospital or the prices charged for a medical act, reveal that an individual is or has been under treatment and may make it possible to establish the nature of the disease. In some cases, the disclosure of information of this kind may be harmful to the individual. It therefore seems reasonable to allow an individual to request that the examinations, medical treatment or operation which he has undergone should not be divulged.

46. It is provided in paragraph 5.3 in fine and 5.4 that the communication of medical data outside the medical or health context will be possible under certain conditions and especially with the proviso that the data subject should give his consent. However, this does not prevent the law from explicitly prohibiting the communication of certain data, even if the data subject does not object. Such is, for example, the tendency with regard to matters concerning artificial insemination.

47. Respect for the purposes of information should not be an obstacle to a possible link between records storing information on the same patients at different times or in different places, in so far as the information exchanged is medically useful and in particular guarantees the continuity of care. However, this linking must take place in accordance with the data bank's specific regulations.

The data subject and his medical record

48. One of the most important principles in the field of data protection is the right of every person to know the information stored about him by other persons.

In the medical field, there are two obstacles to the application of this principle. On the one hand, it may be extremely detrimental to the treatment of a patient if he is given the full facts about his case. Moreover, medical information as such may make little sense to the layman.

49. Paragraph 6 of the recommendation provides as a general rule that every person should be enabled to know of the existence of information about him in a record. Exceptions to this rule should be reduced to a minimum; as an example of such an exception, it might be detrimental for a patient to know that he is on record in a cancer registry.

The data subject should also be enabled to obtain the information itself, but it may be provided that such information should be communicated to him through the intermediary of his physician.

50. A general principle in the field of data protection is that erroneous data must be corrected. The recommendation provides, however, that when knowledge of the error could be relevant to further medical treatment, a record of the erroneous data may be kept. Accordingly, in this specific case, it was decided against "over-writing" that is erasure of an item of information in a record and its replacement with new information.
51. It should be pointed out that if the data subject is incapable (a child, or a legally or mentally incapacitated person), his legal representative will exercise his rights set out in this paragraph, as well as the right of consent mentioned in paragraph 5.

Long-term conservation of data

52. Finally, the recommendation gives attention to a point on which medical data banks must be treated differently from most other types of data banks. As a general rule computerised information should not be stored longer than is strictly necessary, for it is a threat to privacy if information relating to any individual is allowed to accumulate as the years go by. However, the interests of public health and scientific research may justify the long-term conservation of medical data, even after the death of the persons concerned. Specific regulations exist in a number of countries for the conservation of medical archives. The present recommendation, in paragraph 7, permits the long-term conservation of data, provided that adequate safety and privacy safeguards are given.

Professional obligations

53. The use of medical data processing requires the co-operation of many professional people who take part in the design and operation of medical data banks.

But, although professional liability and the doctors' code of ethics are clearly defined, the position of computer experts and other persons involved in the running of data banks should be established more precisely.

At the time of publication of this explanatory memorandum, the Council of Europe's committee of experts on data protection was drawing up more detailed recommendations on the question of rules of conduct for data processing experts.

54. The essential co-operation between the medical profession, data processing experts and other persons sometimes involves the transfer of responsibility. In the case of an error in the transmission of information or the breakdown of the data processing installations assisting the patient, a problem arises concerning the apportionment of liability. Therefore, the duties and responsibilities of the various persons involved should be set out clearly in the regulations.

55. Recorded medical data must be accurate and the contents of records kept up to date. This involves the responsibility of the doctor at the time the data are stored and of the data processing expert when the programme is designed and implemented. Staff responsible for the processing of data are also in charge of installations, programmes and premises, and must, just as members of the medical staff, be required to respect the confidential nature of medical and personal information of which they acquire knowledge in the exercise of their profession.

Extended protection

56. It should be noted that the recommendation does not prevent states from introducing a wider measure of protection to the persons to whom medical data refer.