Explanatory Memorandum
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)

Introduction

1. The impact of data processing technology on various aspects of day to day life, especially personal privacy, has long engaged the attention of the Council of Europe, an intergovernmental organisation which has to its credit the drafting of what is the world's first binding legal instrument in the field of data protection - the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 (ETS No. 108) footnote 1. With reference to specific data processing contexts, a committee of experts mandated by the Council of Europe has laid down detailed principles and guidelines for the protection of privacy based on the provisions of the convention but adapted to suit each context.

2. These principles and guidelines have been embodied in recommendations adopted by the Committee of Ministers and call upon the governments of member states to take account of the solutions offered in their approach to the data protection issues covered.

3. Nine such initiatives have so far been taken in the framework of what is referred to as the "sectoral approach" to data protection:

- Recommendation No. R (81) 1 on regulations for automated medical databanks (23 January 1981);

- Recommendation No. R (83) 10 on the protection of personal data used for scientific research and statistics (23 September 1983);

- Recommendation No. R (85) 20 on the protection of personal data used for the purposes of direct marketing (25 October 1985);

- Recommendation No. R (86) 1 on the protection of personal data used for social security purposes (23 January 1986);

- Recommendation No. R (87) 15 regulating the use of personal data in the police sector (17 September 1987);

- Recommendation No. R (89) 2 on the protection of personal data used for employment purposes (18 January 1989);

- Recommendation No. R (90) 19 on the protection of personal data used for payment or other related operations (13 September 1990);

- Recommendation No. R (91) 10 on the communication to third parties of personal data held by public bodies (9 September 1991);

- Recommendation No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services (7 February 1995).

General comments on the recommendation

4. 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 compilation of medical records.

Medical computer systems meet the new demands of specialisation and teamwork by providing quick and selective access to information on the patient and his/her treatment and thus ensuring continuity in medical care.

5. 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 have many uses in 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.

6. Accordingly, personal health data 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 doctor at the workplace, the doctor of an insurance company, the hospital administrator, social security offices, and so forth.

Usually the recording of medical data occurs in the context of the doctor-patient relationship. It takes the form of a medical record to be used in making the diagnosis and in supervising and treating the patient. In the context of this confidential relationship freely chosen by 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 rules of professional ethics.

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 data subject.

7. 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 depends on a transborder flow of medical data and the setting up of specialised information systems over considerable geographical distances (such as the Eurotransplant organisation for the transplantation of human organs).

8. The needs which medical data processing systems have to satisfy are often contradictory. Information must be readily 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 intensive use of medical data.

9. Certain of the contents of medical files may harm the patient if used outside the doctor-patient relationship. Medical data belong to the most intimate personal sphere. Unauthorised disclosure of personal medical data may therefore lead to various forms of discrimination and even to the violation of fundamental rights.

10. In view of these problems, it has become highly desirable that the operation of every automated medical file should be 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 privacy and dignity are fully respected.

11. Although adoption of such regulations is a matter which comes within the remit of the person or body in charge of each data file (hospital management, faculty of medicine, etc.), it is desirable that they should follow a common pattern and conform to general principles of data protection.

12. It appears advisable that the framework for these regulations should be European in scale. There are two reasons for this.

First, such a European framework will be best suited to the international mobility of people and to international exchanges in the field of medicine.

Secondly, national data protection legislation - including 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, the other, adopted a year later, has established similar principles for the public sector footnote 2. Moreover, in September 1980 the Committee of Ministers adopted a convention on data protection footnote 3, which was opened for signature on 28 January 1981 and which became effective on 1 October 1985. Article 6 of this convention stipulates special safeguards for sensitive personal data, which specifically include information relating to health.

13. In 1990 the Council of Europe's Project Group on Data Protection concluded that Recommendation No. R (81) 1 on regulations for automated medical databanks, whose preparation had commenced in 1976, was no longer in keeping with the rapid development either of medical science or of technology.

Furthermore, since the recommendation was adopted the convention had been signed and implemented and various other sectoral recommendations had been drawn up. It was therefore agreed to carry out a revision of Recommendation No. R (81) 1.

14. It fell to a working party which had been set up by the Project Group on Data Protection to examine current problems raised by data protection in the medical sector. The working party, chaired by

Mr Capcarrere (France), met on seven occasions between February 1990 and July 1992 to "examine the data protection problems created by medical data, including genetic data and data relating to contagious or incurable diseases".

15. Using the same approach as for the drafting of the previous sectoral recommendations, the experts adapted the rules embodied in the convention so as to give them specific application to the protection of medical data.

16. In accordance with the principle laid down in Article 6 of the convention to the effect that "health data" are classified among the special categories of data covered by that provision, the experts have found it necessary that the collection and processing of such data should be attended by appropriate guarantees and safeguards in respect of the data subjects.

17. The definition of appropriate guarantees thus formed the bulk of the working party's activities, which concerned information to the data subject prior to data acquisition, securing the data subject's informed and express consent, and the special case of medical research.

18. The draft produced by the working party was examined by the Project Group on Data Protection in September 1992; it was subsequently revised by the bureau of the project group in November 1992, and in January, March, and September 1993. The project group, chaired by Mr Chalazonitis (Greece), examined it again in May and October 1993.

19. In March 1994 the Steering Committee on Bioethics (CDBI) and the European Health Committee (CDSP) gave their opinions on the draft recommendation.

20. These opinions were examined by the Bureau at its meeting from 22 to 25 March 1994 and proposals to modify the text were made.

21. These proposals were examined by the project group, under the chairmanship of Mr Walter (Switzerland), in June and October 1994.

22. The revised text of the draft recommendation was approved by the project group on 14 October 1994, together with this explanatory memorandum.

23. On 5 December 1994 the draft recommendation and explanatory memorandum were approved by the European Committee on Legal Co-operation, and presented to the Committee of Ministers.

24. The Committee of Ministers passed on the draft to the European Health Committee for a second opinion, which was given on 6 July 1995.

25. In the light of the observations made by the European Health Committee on the one hand, and by the European Commission on behalf of the European Community on the other, the project group revised the draft during its thirtieth and thirty-first meetings (November 1995 and June 1996).

26. The draft recommendation, thus revised, was approved by the Project Group on Data Protection on 7 June 1996, as was the revised explanatory memorandum.

27. On 28 November 1996, both texts were approved by the European Committee on Legal Co-operation.

28. On 13 February 1997, Recommendation No. R (97) 5 on the protection of medical data was adopted by the Committee of Ministers.

Detailed comments on the recommendation

Preamble

29. The preamble contains the considerations which have led the Committee of Ministers to address the recommendation to the governments of the member states footnote 4 .

30. One of these considerations is that compared to other categories of personal data, medical data are also being processed automatically by information systems integrated into medical equipment, as well as outside the health-care sector itself (for example, social security, insurances).

31. Because of this wider use of medical data, and with a view to the fact that under Article 6 of the convention medical data may be processed only if domestic law provides appropriate safeguards, reference is made in this respect to the rights and fundamental freedoms of the individual, and in particular the right to privacy.

32. Moreover, the Committee of Ministers was aware that Recommendation No. R (81) 1 on regulations for automated medical databanks, since its adoption more than fifteen years earlier, had been overtaken by the rapid evolution in respect of medical science as well as of computer technology, and had become obsolete.

Operative part of the recommendation

33. The Committee of Ministers recommends first of all that the governments of the member states take steps to ensure that the principles contained in the appendix are reflected in their law and practice. The wording of this recommendation is flexible, because it is addressed also to those member states which are not yet party to the convention and which have therefore not yet pledged to

take the necessary measures in their domestic law to give effect to the basic principles for data protection.

34. Secondly, governments are recommended to ensure wide circulation of the appendix to the recommendation to all persons who in their profession are called on to collect and/or process medical data.

35. Finally, the Committee of Ministers abrogates the preceding recommendation on regulations for automated, medical databanks. It is clear that the circulation of the present text implies that Recommendation No. R (81) 1 is repealed.

Appendix to the draft recommendation

1. Definitions

36. The definition of "personal data", which follows the definition in the convention as interpreted in the explanatory report to that convention, has already been used in many of the sectoral recommendations adopted by the Committee of Ministers in the field of data protection.

However, with relation to some preceding recommendations, the drafters of the recommendation considered that in view of the developments in computer technology, the aspect of "costs" was no longer a reliable criterion for determining whether an individual was identifiable or not. The definition was also amended to make clear when data could be considered to be anonymous.

37. In the absence of an internationally recognised definition, the drafters of the recommendation opted for the most comprehensive possible definition of "medical data", as it considered the concept of "medical records" in the preceding recommendation overly restrictive in the context of electronic data processing and saw a need to go beyond the discreet relationship between doctor and patient, so as to cover any person likely to keep medical data. It was understood that medical data would equally apply to the past, present and future health of the data subject and to both physical and mental health.

38. The drafters of the recommendation further agreed that under the terms of the recommendation, "medical data" should also include any information - unless it is public knowledge - giving a ready idea of an individual's medical situation, for instance for insurance purposes, such as personal behaviour, sexual lifestyle, general lifestyle, drug abuse, abuse of alcohol and nicotine, and consumption of drugs. This was the reason for including in the definition of medical data the words "manifest and close", that is, having a clear and direct impact on the health situation of the individual.

39. 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 safeguarding anonymity between the donor and the recipient will be covered by this recommendation, since it applies also 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.

40. When medical data appear together with other information in non-medical files, for example insurance, employment or social security files, the protection measures advocated in this recommendation apply also to medical data kept in such files. Apart from the medical data kept therein, such files may raise important problems in respect of individual freedoms; such problems

have been addressed in Recommendation No. R (89) 2 as regards the employment sector and in Recommendation No. R (86) 1 as regards the social security sector.

41. For the purposes of the recommendation, the drafters of the recommendation considered that most of the principles should apply to genetic data as well as to medical data. However, since some principles in the recommendation apply exclusively to genetic data, and in the absence at the time of drafting of a generally accepted definition of "genetic data", they agreed on the definition which appears in Chapter 1. It was understood that this definition did not include the results of an analysis carried out by other means than DNA technology on blood, tissue, hair, sperm, and so forth. Such material might, however, produce genetic data when analysed.

42. Genetic information may result from phenotypic observations, family history studies and laboratory analyses, including observation of genes closely linked to genes causing disease or observation of such genes themselves by DNA technology. Such studies may be conducted to diagnose a pathological condition in individual patients, to evaluate the possibility of future disease in people who are still healthy, or to assess the risk of a person or couple having offspring with a genetic disorder or disease.

43. Genes control many human traits; genetic data are medical data only if they are relevant to health or disease in an individual or his/her relatives.

44. However, following the mandate they had received, the drafters of the recommendation worded the definition in such a way that genetic data are also covered which are not considered to be medical data in the recommendation.

45. Genetic data are collected and stored for prevention, diagnosis, treatment, genetic counselling and risk evaluation as well as for research purposes. As genetic disorders by their very nature are heritable, their presence has implications for all blood relatives, both present and future.

46. Distinctions can be made between the following categories of genetic data:

47. Phenotypic data refer to observations of inherited normal traits, symptoms or signs in a single individual. These observations include clinical observations made by a physician or a physician/geneticist as well as the results of laboratory analyses that can detect inherited or genetically influenced characteristics. Records of phenotypic data relevant to disease are kept in physicians' files and may also be stored in various categories of registers such as driving-licence registers or registers kept for research purposes.

48. Data in physicians' records or registers are genetic data only if they refer to genetically determined, or genetically influenced, traits.

49. Medical history data are in some cases genetic data, namely where information about a given individual indicates that he/she has had symptoms or signs that may reflect the presence of mutant genes.

50. Family data comprise information about a person's parents, uncles, aunts, grandparents, brothers, sisters, children, as well as more distant relatives. Family data are genetic data only to the extent that the disease or trait in a given person is known to be genetically determined or genetically influenced, or if the occurrence of a trait or disease is such that in the given family(ies) it appears to be inherited or influenced by genes, even if it had previously not been suspected that the trait or disease could be of a genetic nature.

51. Family data also comprise information about marriages between related persons and information about numbers of offspring, stillborn children and abortions. Family data are essential for genetic

analyses or normal traits as well as diseases. Records of family data are kept in physicians' files, in medical registers for use in the future in connection with genetic counselling or diagnosis, even in coming generations, or in research registers.

52. Genotypic data comprise information about specific genes at given gene loci in single persons and their relatives. Genotypic data may be the results of phenotypic observations of an individual and his/her relatives. Today, genotypic data may be the results of DNA analyses.

53. Genotypic data include information that a given person is a healthy, heterozygous carrier of a recessive gene which in the homozygous state would cause serious disease, or of an X-linked gene (in a healthy female) which in a male could cause disease (because males have only one X chromosome).

54. Genotypic data may refer either to normal traits or to diseases that are inherited or where a genetic predisposition is of importance (the latter would be the case with several common disorders).

55. Genotypic data relevant to disease will be recorded in physicians' files, in genetic registers for future use in connection with genetic counselling or genetic diagnosis, or in research registers.

56. Genotypic data may be stored in police files if they have been obtained in connection with a crime. Genotypic data may also be recorded in institutions for forensic medicine. This may be the case also for genotypic data obtained in connection with paternity cases. In the last instance, data could also be stored in governmental offices involved in protecting the interest of the children in paternity cases.

57. Genetic information amounting to "genetic data" may also be found in adoption registers, twin registers, published books of a genealogical or biographical nature and many other places. The drafters of the recommendation underlined the importance of the meaning given to the term "genetic data" in the recommendation.

58. The collection and processing of genetic data involves the storage of data concerning third parties. These third parties may be constituted by members of the data subject's genetic line or collateral relatives or members of his/her social family. The drafters agreed to accord an intermediate status to members of the data subject's genetic line so as to distinguish them from third parties in the strict sense of the term and to grant them a hybrid legal protection; they worded the definition of a "genetic line" accordingly.

2. Scope

59. It should be recalled that Article 6 of the convention stipulates that personal data concerning health may not be processed automatically unless domestic law provides appropriate safeguards. Under the 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 automated files not covered by this recommendation.

60. Like the convention, which draws no distinction between the public and private sectors, this recommendation applies to files of medical data in both sectors, since they must meet the same requirements and since there is a frequent transfer of data between the two sectors.

61. The recommendation refers on several occasions to "health-care professionals". The drafters of the recommendation intended this expression to apply to all those persons who, in the exercise of their professions, provide medical care for others.

Having regard to the varied categories of health-care professionals, the drafters of the recommendation felt that it would be difficult to provide in Principle 2.1 an accurate and exhaustive description of

the medical and paramedical personnel who have to collect or process medical data. For example, in certain states social workers would not fall within the category of health-care professionals but might in other countries. The drafters therefore held that the recommendation should apply to any person or body either routinely or occasionally processing medical data by automated means, whether or not for a legitimate reason.

In practice, this means that the principles are applicable to the collection or the processing of medical data for the purpose of medical treatment, the assessment of the health situation or the fitness of a person (for example, for employment, school attendance, national service), preventive care, health consultation, scientific research, rendering social assistance or reimbursement of insurances, as well as for the purpose of identifying an individual.

62. Consequently, since Article 6 of the convention requires appropriate safeguards for the automatic processing of medical data, the drafters of the recommendation agreed that the related principles should also apply to situations where medical data are processed for research purposes (Recommendation No. R (83) 10), in the social security sector (Recommendation No. R (86) 1) and the employment sector (Recommendation No. R (89) 2).

63. The drafters of the recommendation were nevertheless aware of the fact that in some member states domestic law also provides for the collection and processing of medical data in certain sectors other than the health sector, and stipulates appropriate guarantees for this purpose. Consequently Principle 2.1 permits such states not to apply the recommendation to the collection and processing of medical data in those non-medical sectors where national legislation offers other appropriate safeguards for the protection of privacy, in accordance with Article 6 of the convention.

64. In accordance with the definition of "automatic processing" given in Article 2 of the convention, automatic processing within the meaning of the recommendation comprises storage of data, carrying out of logical and/or arithmetical operations on those data, their alteration, conservation, erasure, retrieval or circulation. However, as was noted in paragraph 30 above, automatic processing of medical data might imply the use of information systems other than computers.

65. Like Article 3, paragraph 2.c, of the convention, Principle 2.2 of the recommendation enables any member state to apply the provisions to medical data which are not processed automatically.

On the other hand, states should not allow medical data to be processed by other means simply in order to exclude them from the scope of the recommendation.

3. Respect of privacy

66. In conformity with Article 6 of the convention, the recommendation acknowledges that medical data require even more protection than other non-sensitive personal data. Hence the requirement in Principle 3.1, which does not appear in other sectoral recommendations, that the right of privacy be guaranteed during the collection and processing of medical data, as well as the other rights and fundamental freedoms which might be put at risk. As indicated in paragraph 64 above, the term "processing" also includes the conservation of data.

67. For those reasons, Principle 3.2 recalls the requirement in Article 6 of the convention for appropriate safeguards in the law in so far as the various stages of collection and processing of medical data are concerned.

It should be noted that Principle 3.2 requires such safeguards for the collection of medical data as well. With regard to the processing of such data, it should be recalled that in the terms of the definition (see paragraph 64 above), these safeguards shall be provided for storage of medical data, for their modification, conservation, extraction, diffusion, etc.

68. As one of such safeguards, Principle 3.2 underlines that in principle only health-care professionals, bound by rules of confidentiality, should collect and process medical data, or where necessary persons acting on behalf of health-care professionals, as long as such persons are subject to the same rules.

69. As pointed out in paragraph 61 above, the drafters of the recommendation recognised, however, that in certain member states other professionals, not directly responsible for health care, could collect and process medical data. The third sub-paragraph of Principle 3.2 provides for this possibility, but only on the condition that this category of professionals must abide by confidentiality rules comparable with those imposed on health-care professionals, or that domestic law provides for appropriate safeguards which are as efficient as confidentiality rules, that is, they are efficient enough to guarantee respect of privacy of the data subject. Principle 3.2 therefore complements Principle 10.4 of Recommendation No. R (89) 2 on the protection of personal data used for employment purposes, which requires that data covered by medical secrecy should be stored only by personnel bound by the rules on medical secrecy.

4. Collection and processing of medical data

70. Once again, with a view to the sensitive nature of medical data, Principle 4.1 recalls the provisions in Article 5 of the convention: the collection and processing must be fair and lawful, and for specific purposes only. These requirements are elaborated further in Chapter 4.

71. The principle of fair collection is made more explicit in Principle 4.2: medical data must, in normal conditions, be obtained from the data subject himself/herself. This principle therefore concerns the "disclosure" of these data by the data subject himself/herself, and not "communication" of medical data by a third party (for example, the doctor).

72. It is obvious that this rule cannot always be applied; in such cases other sources of information may be consulted only if this is necessary to achieve the purpose for which the data are to be processed (for example, medical treatment) or if the data subject cannot provide the data himself/herself. But in any case, the collection of medical data must be in accordance with the related provisions in Chapter 4 (see paragraphs 73-104 hereafter), Chapter 6 (see Consent, paragraphs 129-142 hereafter) and Chapter 7 (see Communication, paragraphs 143-152 hereafter).

73. After the provisions indicating how medical data should be collected (Principle 4.1) and from whom (Principle 4.2), Principle 4.3 lays down when medical data may be collected or processed. They may be collected, if provided for by law, where there is a contractual obligation to do so if this is necessary for the establishment of a legal claim or when the data subject has given his/her consent. Principle 4.3 does not constitute a derogation from Principle 3.2, but sets conditions for the legitimacy of the collection or processing.

74. Medical data may also be collected from the data subject or from other sources if this is provided for by the law for one of the purposes set out in Principle 4.3.a: public health, the prevention of a real danger or the suppression of a specific criminal offence, or another important public interest.

When medical data are collected and processed, the appropriate safeguards described in Principle 3 shall be provided by domestic law.

Furthermore, medical data may be collected and processed if permitted by law for the purposes set out in Principle 4.3.b: for preventive medical purposes or for diagnostic or therapeutic purposes, or to safeguard the vital interests of a data subject, or with a view to respecting specific contractual obligations, or with a view to the establishment, exercise or defence of a legal claim. In accordance with principle 4.3.c, medical data may also be collected and processed if the data subject has given his/her consent for one or more purposes in so far as domestic law does not provide otherwise.

Collection and processing of medical data for the establishment, exercise or defence of a legal claim may be carried out only when a specific case occurs, for example a conflict between a doctor and a patient about treatment, allowing the doctor to communicate data to his/her lawyer in order to defend himself/herself in a lawsuit. Collection "in anticipation" is not lawful.

The physical or legal incapacity of a data subject to give his/her consent gives rise to a situation where medical data may be collected, processed or communicated to safeguard the vital interests of this person (Principle 4.3.b.ii and 7.3.b.ii).

When medical data are collected and processed in the context of contractual obligations (Principle 4.3.b.iii and 7.3.b.iii), member states of the European Union will, after transposition of the community directive into their national legislation, be able to make use of this option only in the context of labour law; for the other member states of the Council of Europe these principles may be taken into consideration in other fields, such as sport, training or insurance.

The drafters of the recommendation felt that in each of these conditions medical data may be collected and processed if the law - including that in common-law countries, in common law or in statute - explicitly provides for it. If the law provides for the collection, without giving the appropriate safeguards required under Article 6 of the convention, a derogation is in fact made under Article 9 of the convention. The conditions set out in that article must be respected, that is, the collection must constitute a necessary measure in a democratic society in the interest of protecting state security, public safety, the monetary interests of the state or the suppression of criminal offences, or of protecting the data subject or the rights and freedoms of others.

75. For the purposes of the recommendation, the authors thought that the expression "the law" should be understood in the sense given to it in the case-law of the European Court of Human Rights. In particular, it must be precise, foreseeable and accessible.

76. The words "if provided for by law" also cover cases where collection and processing are laid down by law. If medical data may be collected and processed as a consequence of an obligation under the law (for example, in the field of social insurances to obtain invalidity pension, or in the field of epidemic prevention), the drafters of the recommendation have trusted the legislator to take account of the other requirements in Article 9 of the convention, that is, that the processing constitutes a necessary measure in a democratic society in the interests of protecting state security, public safety, the monetary interests of the state or the suppression of criminal offences, or protecting the data subject or the rights and freedoms of others.

77. Medical data may therefore be collected without consent, if the law provides for this, "for the purposes of" (that is, in the interest of) public health; this purpose is in line with the derogation for reasons of public safety in Article 9 of the convention. It should also be noted that the words "in the interest of public health" include the management of health services.

78. The drafters of the recommendation agreed that medical data could furthermore be collected without consent, if provided for by law, for the prevention of a real danger or the suppression of a specific criminal offence. Rather than the terminology used in Article 9 of the convention, they

preferred the wording used in Recommendation No. R (87) 15 regulating the use of personal data in the police sector. Principle 2.1 of this recommendation excludes an open-ended, indiscriminate collection of data by the police. It expresses a qualitative and quantitative approach to Article 5.c of the convention which stipulates that personal data must be adequate, relevant and not excessive in relation to the purposes for which they are stored. Given that Article 9.a of the convention allows a derogation from this principle in regard to the "suppression of criminal offences", Principle 2.1 of the recommendation attempts to fix the boundaries to this exception by limiting the collection of personal data to such as are necessary for the prevention of a real danger or the suppression of a specific criminal offence, unless domestic law clearly authorises wider police powers to gather information. "Real danger" is to be understood as not being restricted to a specific offence or offender but includes any circumstances where there is reasonable suspicion that serious criminal offences have been or might be committed to the exclusion of unsupported speculative possibilities. Moreover, processing of genetic data for the requirements of legal proceedings or a criminal enquiry is governed by Principle 4.7 (see paragraph 95 below).

79. Apart from public health, a real danger or the suppression of a criminal offence, there may be other important public interests at stake. Principle 4.3.a.iii permits the law to provide for the collection and processing of medical data to protect such interests.

80. It may be that the data subject is not in a position to give his/her consent. If the law provides for this, the data may be collected and processed to safeguard vital interests of the data subject, or of a third person, that is, to preserve the physical or mental integrity of either the data subject or somebody else including, in the case of genetic data, a member of the data subject's genetic line. This implies that medical data may be collected and processed without the consent of the data subject for preventive medical purposes, or for diagnostic or therapeutic purposes, with respect to the data subject or to a member of the genetic line, or even a third person, in order to protect an interest which is essential for the data subject's life.

81. Principle 4.3 permits also the collection and processing of medical data if they are necessary in order to respect any obligation arising from a contract, on condition however that domestic law permits it. The authors of the recommendation felt that, especially in labour law, a contractual obligation or a contractual right should be able to give rise to collection or processing of medical data, as the data subject had already given his/her consent when the contract was concluded.

82. Principle 4.3 also takes account of lawsuits; medical data may be collected and processed without the consent of the data subject if permitted by law and if this collection or processing is necessary for the establishment of a legal right. It should be recalled nevertheless that, by virtue of Principle 4.7, processing of genetic data for the requirements of a legal procedure should be covered by a specific law providing the appropriate safeguards.

83. Apart from any legal provision or obligation, medical data may also be collected and processed if the data subject - or his/her legal representative - has given consent, unless domestic law opposes this. The drafters of the recommendation were aware that, from the point of view of protection of medical data, consent of the data subject gives fewer guarantees than legal obligations or legal provisions which - by virtue of Article 6 of the convention - should be accompanied by appropriate safeguards. In Chapter 6 of the recommendation, the conditions for such consent and the possible derogations are elaborated further.

84. Medical data collected by a health-care professional for preventive medical purposes or for diagnostic or for therapeutical purposes may, after the specific medical care, also be necessary to accomplish other services in the interest of the patient; for example, the chemist will have to supply

him/her with the prescribed medicine, the administrative service of the hospital will have to make out the bill, or the social security services will have to organise the reimbursement of the expenses incurred. The authors of the recommendation felt that the purpose of processing by such "health services" (which do not cover insurance companies acting on a contractual basis) is compatible with the purpose of the collection of these medical data. Principle 4.4 accordingly permits processing of medical data for these health services, on condition that the processing is carried out in the interests of the patient.

85. This type of health service may be managed by the health-care professional who collected the medical data, or by someone else. In the latter case, the necessary medical data may be communicated by the health-care professional in accordance with Principles 7.2 and 7.3 (see paragraphs 144 and 145 below).

Unborn Children

86. The protection of the medical data of the unborn child, with a view to the protection of its privacy once it is born, raises specific questions, of in particular, an ethical nature, which are beyond the scope of this recommendation.

87. When drafting principles 4.5 and 4.6, the principal concern of the drafters of the recommendation was not to establish parental authority, but rather to ensure that a child's medical data were not "public" at the time of its birth.

In the absence of a generally accepted legal rule on when an unborn child can be considered to be a person, the drafters of the recommendation were of the opinion that measures should be taken to ensure the protection of the medical data of a child which had been collected and processed before its birth, and that therefore the unborn child should be protected in a way similar to the protection of the medical data of a child after its birth. For example, this may be achieved by considering data of the unborn child to be the personal data of the mother. This requirement is confirmed in Principle 4.5.

88. Following the trend in family law in the member states, the drafters of the recommendation concluded in Principle 4.6 that unless domestic law provides otherwise, the holders of parental responsibilities of the future child should be entitled to act on behalf of the unborn child as a data subject.

It was understood that in the exercise of the rights of access to and rectification of the medical data of the unborn child, the interests of the mother must be duly taken into account.

Genetic data

89. In spite of the specific nature of genetic data (see paragraphs 41-58 above), the drafters of the recommendation considered that the conditions for their collection and processing should be the same as those for the collection and processing of medical data, set out in Principle 4.3.

90. In this connection, the drafters of the recommendation were aware that the collection and processing of genetic data may be necessary in the interests not only of the protection of public health, but also the promotion of public health, since genetic analyses might reveal health risks for future generations. They were aware, however, that this possibility should not lead to a proliferation of genetic databanks, or an abuse of genetic data.

91. Principle 4.1, inspired by Article 5 of the convention, implies that genetic data may be processed only for purposes compatible with the purposes for which they were collected, and on the same conditions. The drafters of the recommendation did not include a requirement that genetic data should not be used for artificial modifications of the genetic heritage of data subjects, cloning or the

selection of individuals, since such requirement would seem to be outside the scope of the recommendation, and is, in any case, covered by the principle of compatible purposes.

92. Genetic data collected and processed for diagnosis or medical or preventive treatment or for scientific research purposes, should only be used, in the first instance, for these specific purposes or to enable the data subject to take a decision whether or not to undergo treatment; the same principle applies when the data were collected with a view to procreation. Principle 4.7 is a logical consequence of the general principle of purpose specification; to use or re-use such data for other purposes should not be allowed. Principle 4.7 also applies when genetic analysis is carried out to establish whether a person can procreate without risk to the health of his/her future children. In this respect, Principle 4.7 does not aim at establishing an ethical norm on whether or not procreation should be preceded by genetic analysis; the principle merely requires that if genetic data are collected for that purpose in accordance with domestic law or the existing ethical standards, they may be used only to facilitate the data subject's decision.

93. In defining Principle 4.7 the drafters of the recommendation paid special attention to the use of genetic data for scientific research; in this context they confirmed that such research would be ruled by Chapter 12 "Scientific research". It was agreed that secondary use for scientific research of genetic data which had been collected for other purposes would not be incompatible with these initial purposes, as long as the conditions in Chapter 12 were respected, in particular Principle 12.2 (see paragraphs 200-209 hereafter) and Principle 12.3 (paragraph 209).

94. Principle 4.7, which applies to scientific research in general, is followed by two principles aimed more specifically at situations where genetic analysis may be carried out with a specific aim.

95. Although the analysis of deoxyribonucleic acid (DNA) within the framework of criminal justice is regulated in Recommendation No. R (92) 1, adopted by the Committee of Ministers on 10 February 1992, the drafters of the recommendation considered it useful to include in this recommendation a provision on the protection of genetic data processed for the purpose of criminal investigations, which also covers analysis of such data for the requirements of judicial procedures.

96. The expression "judicial procedure" is not used in the same way in member states. The drafters of the recommendation wished Principle 4.8 to apply to any procedure before the courts, whether initiated under civil or criminal law, where the judicial proceedings may have recourse to genetic analysis of one or more persons.

97. Consequently, Principle 4.8 requires a specific law for the processing of genetic data for judicial procedures and criminal investigations. By "specific law" is understood either a specific provision of the data protection act, or a specific provision in penal law, as long as they refer to the use of genetic data for the purpose of criminal investigations. This requirement is a logical consequence of Article 6 of the convention which imposes appropriate safeguards in domestic law for the processing of any sensitive data. The principle of compatibility of purposes also applies here: data collected and processed in the framework of judicial procedures and criminal investigations shall be used only for the original purposes and not for other purposes, in particular not to determine other characteristics of the data subject (see paragraph 78 above).

98. The second paragraph of Principle 4.8 is intended to define these purposes. Genetic data processed for the needs of a judicial procedure, for example a paternity suit, should be used only to establish whether or not there is a genetic link between the child and the alleged father. In the same way, in a criminal investigation genetic data should be used only in order to prevent a real danger or suppress a criminal offence.

99. It was considered that the proof of guilt or innocence, even on the basis of evidence supplied by genetic analyses, would be beyond the scope of this recommendation.

100. Principle 4.9 aims at regulating the use of genetic data for purposes other than diagnosis, therapeutic or preventive treatment, scientific research or criminal investigations. This use can only be allowed in principle for health reasons and to avoid every serious risk for the health of the data subject or for a third person. However, in the case of the collection and processing of genetic data in order to predict illness, the recommendation requires the existence of an overriding interest and appropriate safeguards provided for by law in view of the various risks inherent in the collection and processing of genetic data, in particular the risk of discrimination (as far as reference to law is concerned, in view of the case-law of the organs of the European Convention on Human Rights, see paragraph 75 of the present explanatory memorandum).

101. It should be recalled that the conditions for lawfulness laid down in Principle 4.3 also apply to the collection and processing of genetic data.

102. Principle 4.10 adds a supplementary condition for genetic data to be collected and processed: the purpose of collection and processing must be health protection and in particular the prevention of any serious harm to the data subject or a third person.

103. The drafters of the recommendation emphasised that a candidate for employment, an insurance contract or other services or activities should not be forced to undergo a genetic analysis, by making the employment or the insurance dependent on such analysis, unless such dependence is explicitly provided for by law and the analysis is necessary for the protection of the data subject or a third party (for example work with dangerous substances).

104. Principle 4.9 is even more specific with regard to the collection and processing of genetic data with a view to predicting illness. Such data may be collected and processed if the interest in doing so overrides the data subject's interest in not having his/her genetic data collected and processed (for example a collective interest) and if domestic law has provided appropriate safeguards.

It was understood that such overriding interest should be in accordance with the related criteria set out in Principle 4.3.

5. Informing data subjects

105. One of the means to ensure that medical data are obtained and processed fairly and lawfully, as required under Article 5 paragraph a of the convention, is to inform the data subject whose data are collected of a number of elements. These elements are listed in Principle 5.1.

106. It is obvious that such provision of information is indispensable when the data subject is required to give his/her "informed" consent (see paragraph 130 hereafter).

107. But even in cases where his/her consent is not required - that is, when the collection and processing of medical data follow an obligation under the law or under a contract, are provided for or authorised by law, or when the consent requirement is dispensed with - the recommendation provides that the data subject is entitled to relevant information. Although the drafters of the recommendation agreed that as a general rule Principle 5.1 should be strict, they admitted two kinds of derogation. First of all, Principle 5.6 allows for derogations to be made for certain reasons of public interest, for protection of the data subject or a third person, or in medical emergencies. Secondly, information on the various elements listed under a, b, c and d has to be supplied only in so far as it is relevant (see paragraphs 115, 116 and 124 hereafter).

108. Principle 5.1 identifies the following elements on which the data subject must be informed:

a. the existence of a file containing his/her medical data, and the type of data collected or to be collected: in most cases, it may also be necessary to collect personal data from the data subject other than medical data;

b. the purpose or purposes for which the data are or will be processed: apart from medical purposes, the data may have to be processed for other purposes, for example for reimbursement of expenses, for research or for statistics;

c. where applicable, the individuals or bodies from whom the data are or will be collected: Principle 4.2 provides for the possibility to obtain medical data from other sources;

d. the persons or bodies to whom and the purposes for which they may be communicated: apart from health-care professionals, other professionals, including chemists, social security officials, and family members or legal representatives, may have to be informed of certain medical data for specific purposes;

e. the possibilities for the data subject to refuse or withdraw his/her consent, if possible, and the consequences of such withdrawal: if the data subject has the possibility to refuse or withdraw his consent, it is clear that any such refusal or withdrawal can only apply to his/her own medical data. It should also be made clear that the obligation to inform the data subject in no way prejudices the existence of the right to refuse or withdraw consent;

f. the identity of the file controller and, where appropriate, of his/her representative as well as the conditions under which the rights of access and of rectification may be exercised.

In accordance with Article 8, paragraph a, Principle 5.1 requires that the data subject be informed of the identity of the person responsible for processing his/her medical data, or of his/her representative.

These conditions for the exercise of rights of access and rectification are laid down in Chapter 8 of the recommendation.

109. According to Principle 5.2 the information should be provided before the data are collected. This is not always possible, for example when the data cannot be collected from the data subject himself/herself. In such cases he/she must at least be informed, as soon as possible, that his/her data have been collected and, in so far as necessary and possible (for example if the data subject is already aware, or is not in a position to understand) the relevant elements listed in Principle 5.1 must be provided.

110. The drafters of the recommendation agreed that it be left to each member state to determine ways and means to supply the information.

111. Provision of the information on the elements above may be partly of a general nature, that is, some information applies to all patients who are treated by a given health-care professional or in a given health-care institution. For instance, the public at large should be given general notice in advance of any plans involving the introduction of automatic processing systems for medical data. Such "collective" information may be given by the most efficient and practical means, for example on posters, in leaflets or in public registers.

112. Other parts of the information may concern the health situation of a given individual, that is, apply only to the patient and his/her particular medical data. In such cases Principle 5.3 requires this sort of information to be appropriate and adapted to the circumstances and in accordance with the rules of deontology. The information and the method of supplying it should then be specially aimed

at the individual and his/her capacities to understand it: the information must be "individualised" and preferably be given to each data subject individually.

113. In the same way, the relationship of trust between the patient and doctor may have consequences for the content and form of the information. "Information (...) appropriate and adapted to the circumstances" also takes account of this relationship, and provides, for example, that the doctor should give supplementary information if his/her patient requests it.

114. The drafters of the recommendation underlined, however, that any relevant information, whether provided collectively or individually, is equally important, and should in all cases be appropriate.

115. The drafters of the recommendation also acknowledged that on some occasions the data subject may not have to be told some or all of the elements referred to in Principle 5.1, either because these elements are obvious to him/her from the context in which the medical data are collected, without the need for further explanation, or because he/she has already been properly informed of these elements on a previous occasion.

116. "Information (...) adapted to the circumstances" can imply that the requirement of information may partly be waived in respect of certain elements, if the health-care professional in charge of the treatment believes that knowledge of any of these elements might harm the person whose data are to be collected. In such a case he/she may either postpone the providing of information, or supply it through another medical doctor, designated by the patient. The drafters of the recommendation saw no need to include a specific principle on this possibility.

117. All these provisions, however, only allow the right to information to be adapted, not to restrict the information.

118. The data subject need not be informed by the actual person in charge of processing the data. However, the person in charge of the medical treatment should ascertain himself/herself that the patient has had the opportunity to obtain in particular the "individualised" information. The drafters of the recommendation were aware of the difficulties which the medical doctor might meet in practice; they agreed therefore that he/she should see to it that the data subject has had access to the information, unless this is manifestly unreasonable or impracticable.

119. A genetic analysis may produce other results than the information sought; such unexpected findings, that is, findings which are not causally linked to the aim of the analysis, may cause harm to the data subject, or he/she might prefer not to know them. Moreover, the drafters of the recommendation felt that developments in genetic research are too recent and too significant to expect the uninitiated to be as familiar with the potential results as with those of a traditional medical examination. Principle 5.4 recommends therefore prior informing of the data subject on the objectives of the genetic analysis, and on the possibility of finding more. If necessary, this provision of information may be deferred.

120. As indicated in paragraph 41 above, blood tests are not in themselves genetic analyses. The drafters of the recommendation thought that establishing the rhesus factor should not be considered as an analysis of the human genome, to which Principle 5.4 applies.

121. It is clear that information can be supplied only to persons capable of understanding; Principle 5.5 provides for the information to be given to the person legally recognised to act in the interests of a data subject who is legally incapacitated.

Under "legally incapacitated persons" the drafters of the recommendation understood any person whose situation gives rise to his/her consent being defective under domestic law.

122. However, in some member states domestic law permits certain incapacitated persons to act on their own behalf if they are capable of free decision (for example, on medical contraception). In such cases, Principle 5.5 allows the information to be given to the data subject himself/herself.

123. The drafters of the recommendation felt that the "information (...) appropriate and adapted to the circumstances" required in Principle 5.3 should apply equally to de facto incapacitated adults. Rather than create a supplementary category of derogations from the right to information, with the risk of abuse, the drafters wished to place confidence in health-care professionals.

The recommendation encourages the provision of information to legally incapacitated persons who are, however, capable of understanding it; as will be seen in Principle 6.4, account should be taken of the opinion which such persons express, unless this is contrary to domestic law.

124. As pointed out in paragraph 107 above, the drafters of the recommendation acknowledged that under certain conditions medical data could be collected without informing the data subject of each of these elements. These conditions are listed exhaustively in Principle 5.6 of the recommendation. The drafters agreed that such derogation from the information requirement could not be made when access to the data was refused, limited or delayed (see paragraph 156 hereafter).

125. It was emphasised, however, that any derogation would in general apply only to the requirement of provision of information prior to the collection of data; to the extent possible the obligation to inform the data subject after the collection would remain valid, as would the general obligation to obtain his/her consent before processing the data.

126. In the spirit of Article 6 of the convention, which requires appropriate safeguards for the processing of medical data, the drafters of the recommendation, in respect of the requirements of individualised information and consent (see also paragraph 133 hereafter), narrowed in Principle 5.6.a the possibilities for providing for derogations and restrictions which are otherwise allowed under Article 9 of the convention. In this way such derogations and restrictions are allowed only if provided for by law, and if this constitutes a necessary measure in a democratic society in order to prevent a real danger or to suppress a specific criminal offence (see paragraph 78 above), to protect the data subject or the rights and freedoms of others, including relatives of the data subject, or for reasons of public health (see paragraph 77 above).

127. It may be in the interest of the data subject if in emergencies those medical data which the health-care professional considers necessary for treatment are collected and processed before he/she is informed of this collection (Principle 5.6.b).

128. Subject to paragraph 119 above, it should be emphasised that Principle 5.6 does not permit derogation from the right to information before collection of genetic data as laid down in Principle 5.4; indeed, the drafters of the recommendation felt that collection of genetic data should always be preceded by the informing of the data subject, unless the urgency of this collection requires the deferment of such provision of information.

6. Consent

129. One of the conditions on which medical data may be collected and processed is that the data subject has given his/her consent in so far as he/she is capable of doing so. As these data are regarded as sensitive data within the meaning of Article 6 of the convention, Principle 6.1 requires

that the consent be "free, express and informed". It may be obtained in coded form (as with plurifunctional cards, for instance).

130. Free, express and informed consent given in writing is a requirement laid down in the recommendations on data protection in other sectors; for the processing of medical data, such consent need not be written; it can also be given orally, or by means of a recording, provided that the desired purpose of authenticating the data subject's agreement is achieved.

131. Consent is "informed" if the data subject is informed in particular of the purposes involved and the identity of the data controller. Consent is "free" if the data subject has the possibility to refuse his/her consent, to withdraw it or to modify the terms and conditions of consent.

132. The drafters of the recommendation were aware that the principle of free consent implied the possibility of withdrawal. However, it was accepted that a provision on the possibility for the data subject to withdraw consent at any time would lead to too many practical problems (for example, in a fully automated hospital). It should be clear, however, that if domestic law makes social benefits dependent on the processing of medical data, the data subject must accept that withdrawal of consent might imply the loss of these benefits.

133. The drafters of the recommendation also acknowledged that under certain conditions medical data could be processed without the data subject's free, express and informed consent. These conditions are listed exhaustively in the recommendation.

134. As regards the collection of medical data in the course of a consultation or treatment for preventive, diagnostic or therapeutic purposes by a doctor, and which the data subject has freely chosen, the drafters of the recommendation felt that the consent of the patient need not be expressed if the data were indeed to be processed only for the provision of care to the patient. Principle 4.3.b.i provides the legal basis for processing medical data in the context of the management of a medical service operating in his/her interest (see paragraph 84 above).

135. The observations made under paragraph 134 also apply to the auxiliary staff of the person in charge of the treatment, for example nurses and secretaries, and members of other health-care professions who assist the attending physician (radiographer, scanner).

136. Principle 6.2 provides that after genetic analysis the data subject should only be informed of the results in so far as these correspond to the objectives of the consultation, of the diagnosis, or of the treatment, unless the data subject himself/herself has asked for more information (see Principle 8.4 hereafter). In other words, the content of the consent is decisive for access to the results of the analysis (see paragraph 164 hereafter).

137. Principle 6.3 provides that if a legally incapacitated person cannot decide freely, nor act on his/her own behalf, consent for the processing of his/her medical data must be given by the person legally entitled to act in the interest of the incapacitated data subject or by any other authority, body or person designated by the law.

138. Up to the age of legal capacity, the parents of a minor are legally competent to fulfil the required conditions of consent on his/her behalf. Where there are no parents, the court appoints a guardian to perform this function. The same applies to any other person or body recognised by domestic law as being legally competent to manage the affairs of the minor.

139. As to adults de facto incapable of giving their consent, for instance for reasons of mental illness, the drafters of the recommendation considered that the national legal systems or courts

should appoint a legal representative or other authority, body or person able to give consent on behalf of the incapacitated person.

140. Consent by the legal representative or other authority, body or person designated by law, can only be given instead of the consent required from the data subject, and on the same conditions.

However, if in accordance with Principle 5.5, the incapacitated person has been informed (see paragraph 122 above), his/her wish to accept, or not, collection and processing of his/her medical data should be taken into account unless this is contrary to the law.

141. In medical emergency situations, medical data may be collected and processed even without the consent of the data subject. This follows from Principle 4.3, sub-paragraph a.iv (see paragraph 80 above). However, the drafters of the recommendation underlined that any decision to proceed to the collection and processing of medical data without consent of the data subject should not be taken for reasons of interest to persons other than the patient. For example, a decision to disclose health data for medical research purposes should not be taken by the researchers themselves; an independent third party should be found, for instance a family member. Furthermore, it is clear that in such situations only those data may be collected and processed which are necessary for the medical treatment, and only as long as the data subject is not able to give consent.

142. The drafters of the recommendation agreed that there was no need for a special principle explicitly dispensing the person in charge of medical treatment from the requirement to seek consent when this might cause serious harm to the data subject. The consent is dispensed with by virtue of Principle 4.3.b.i.

Moreover, Principle 5.6 allows information to be withheld from the data subject for his/her own protection; any consent required in such circumstances would therefore not be "informed".

7. Communication

143. It is obvious that medical data, one of the categories of sensitive data for which the convention requires special protection, should not be communicated outside the medical context in which they were collected, unless they are made anonymous (in which case the data no longer fall under the definition of personal data).

There are however certain circumstances under which relevant medical data must be disclosed to other persons or bodies which, while not in charge of the medical treatment of the data subject, act otherwise in his/her direct interest (for example social security services), or are in charge of medical research. In the latter case, the provisions under Chapter 12 apply as well as the provisions in this chapter. Principle 7.3 defines four alternative conditions for such disclosure.

144. As is clear from Principle 7.3, medical data may be communicated under certain conditions and also outside the medical sector. However, Principle 7.2 introduces, as one of the appropriate safeguards referred to in Article 6 of the convention, the preliminary condition that such communication may only be made to persons bound by confidentiality, unless the domestic law provides for other safeguards. The rules of confidentiality are medical secrecy, for the medical sector or comparable rules for other sectors. In all cases, the person who receives the data should be subject to the principles of the recommendation.

145. Principle 7.3 permits communication of medical data in so far as they are relevant to attaining the objective for which they are communicated, even without the knowledge of the data subject and even for a purpose other than that for which the data were collected. The drafters of the

recommendation have consequently taken care to specify the four alternative conditions under which such communication may take place.

146. First of all, the drafters of the recommendation based paragraph a on the conditions imposed in Article 9 of the convention for any derogation from the protection of sensitive data. Communication of medical data may therefore take place if it is provided for by law and constitutes a necessary measure in a democratic society for one of the following objectives:

a. reasons of public health (for example, in the case of contagious diseases);

b. protection of the data subject himself/herself (for example where communication is clearly in his/her own interest);

c. protection of a member of the genetic line (for example where the results of a genetic analysis point to a serious risk for another member of the genetic line; see paragraph 151 below);

d. protection of the rights and liberties of others if respect of these rights and liberties clearly overrides the interests of the data subject (for example in the case of contagious disease);

e. respect of contractual obligations with regard to labour law (for example in cases of sickness of the employee);

f. prevention of a real danger or suppression of a specific criminal offence (for example the search for a wounded criminal in a hospital; see also paragraph 78 above);

g. any other important public interest (for example state security).

147. The drafters of the recommendation agreed that the expression "measure which is necessary in a democratic society" permits communication in the case of an interest which overrides that of the data subject.

148. Secondly, medical data may be communicated if such communication is necessary for the proof, exercise or defence of a right in court. As this concerns communication of sensitive data, in the interest of a third person, without the knowledge of the data subject and for purposes incompatible with those of collection, the drafters of the recommendation emphasised that the proof, exercise or defence of a right in court shall prevail over the right to privacy of the data subject.

The physical and legal incapacity of a data subject to give his/her consent gives rise to a situation where medical data may be collected, processed or communicated to safeguard the vital interests of this person (Principles 4.3.b.ii and 7.3.b.ii).

With regard to collection of medical data in the context of contractual obligations (7.3.b.iii and 4.3.b.iii), member states of the European Union may use this option only in the context of labour law; in other member states of the Council of Europe these principles may be taken into consideration in other fields, such as sport, training or insurance.

149. Thirdly, medical data may be communicated if the data subject - or his/her legal representative - has given his/her consent and domestic law does not provide otherwise. By virtue of Principle 6.1 this consent should be free, express and informed (that is, be preceded by prior provision of information as required in Principle 5.1); consent is not required when the conditions described in Principle 7.3.d are fulfilled.

150. Consent may be given for a clearly defined purpose, or the communication may be made for several purposes at once, for example for medical research in general. It should be noted that such

communication, based on consent, is not necessarily accompanied by the appropriate guarantees required by Article 6 for communication in accordance with domestic law.

Such communication is, however, dependent on domestic law to take account of member states where medical secrecy rules exclude any disclosure of medical data by health-care professionals, even if the data subject consents. Such rules vary from one state to another.

151. Fourthly, medical data may be communicated where the following cumulative conditions have been fulfilled:

a. the data subject (or his/her representative) has not opposed the (non-obligatory) communication;

b. domestic law is not opposed to it;

c. the data had been collected in a preventive, diagnostic or therapeutic context freely chosen by the data subject;

d. the purposes of communication and preceding processing are not incompatible. The drafters of the recommendation felt that such compatibility exists where the data are communicated for treatment of the patient, or to manage a medical service acting in his/her interest (see paragraph 84 above).

152. The drafters of the recommendation acknowledged that the questions raised by disclosure of genetic data would seem to be of an ethical nature and beyond the scope of this recommendation. From the point of view of protection of personal data they considered that the person subjected to a genetic analysis should be encouraged to advise the other members of his/her genetic line to ask for genetic consultation when the resulting information needs confirmation or reveals the existence of a serious risk for their health.

Furthermore, and depending on national legislation and professional rules of conduct, if the health of a blood relative (on the mother's or father's side) is exposed to a serious and imminent risk, the health-care professional involved should be allowed to inform that member, even if the person subject to the original genetic analysis refuses to give his/her consent or this consent cannot be obtained. The data subject should be informed of this.

8. Rights of the data subject

153. One of the most important principles in the field of data protection, confirmed in Article 8 of the convention, is the right of every person to know the information about him/her stored by other persons.

In the medical field there are three main obstacles to the application of this principle. Firstly, it may be extremely detrimental to the treatment of a patient if he/she is given the full facts about his/her case. Secondly, medical information as such may make little sense to the layman. And thirdly, medical data, and in particular genetic data, may concern also persons other than the data subject.

Rights of access and rectification

154. Principle 8.1 summarises, in respect of medical data, the provisions under Article 8, paragraphs a and b, of the convention: as a general rule, every person shall be enabled to have access to information about himself/herself in a medical file and implicitly to know of its existence. 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/she is on record in a cancer register.

For this reason, Principle 8.1 leaves the option that the right of access be exercised indirectly (see the following paragraph); in that case, and unless this would be contrary to domestic law, the data subject should specify this and be enabled to designate for this purpose a person of his/her choice, who should be given full access.

155. In some member states, domestic law does not enable the data subject to have direct access to his/her medical data (for example in accordance with the rules of medical secrecy), which in fact constitutes a derogation under Article 9 of the convention. If, however, this right exists and the data subject does not wish to exercise it himself/herself, he/she should be enabled to designate a person - in accordance with domestic law - to have access. Depending on the law in force, such a person may be a medical doctor or other health-care professional, a relative or any other person of the data subject's choice.

156. As is the case with "individualised" information (paragraph 112 above), the data subject must be enabled, to the extent possible, to understand the information to which he/she has access. This does not mean that medical data must be stored in an intelligible form; in many cases information will be coded, for example diagnostic groups. What is important is that the information is accessible to the data subject - or the person of his/her choice - in a form which can be understood by him/her.

157. Like Article 9 of the convention, Principle 8.2 allows for derogations to be made from the right of access to medical data if the law provides for such refusal, limitation or delay. Principle 8.2 is also based on the general principle of proportionality; access to medical data cannot be refused, limited or delayed except to the extent to which it is necessary: each case should be considered on its own merits.

158. Firstly, the right of access may be refused, limited or delayed if this constitutes a measure which is necessary in a democratic society to protect state security, public safety or for the suppression of criminal offences. The drafters of the recommendation felt that access to medical data should not be restricted to protect the monetary interests of the state.

159. Secondly, access to medical data may also be refused, limited or delayed if it is likely to cause serious harm to the data subject's physical or mental health; paragraph 8.2.b recognises "the right not to know". In such cases it would, however, be desirable for access to be given indirectly (see paragraph 152 above), and in any case as soon as the risk of harm no longer exists, access must be given.

160. Thirdly, access may be refused, limited or delayed if it would reveal information on third parties, and the protection of the personal data of this third party would override the interest of the data subject to have access to his/her own medical data. Moreover, the drafters of the recommendation provided also in paragraph c for the possibility to refuse, limit or delay access to genetic data when this might cause serious harm to a member of the genetic line, or to a person who has a direct link with this line, for example a presumed family member who appears not to be a member of the genetic line, or a presumed outsider who turns out to belong to the family.

161. Finally, paragraph d of Principle 8.2 opens the possibility, provided for in Article 9, paragraph 3, of the convention, of restricting the right of access to data used for statistical purposes or scientific research, where this restriction creates no risk of infringement of the privacy of data subjects, for example where safeguards provide that the data will not be used for taking decisions about the data subject.

162. Under Article 8 of the convention, the right of access to one's personal data goes hand in hand with the data subject's right to obtain, on certain conditions, rectification or erasure of his/her data. A

general principle of data protection is that data must be corrected or erased if they are erroneous. In the medical sector, however, the exercise of this right of rectification or erasure may sometimes raise problems of a specific nature.

163. Principle 8.3 therefore allows the data subject to ask for rectification of such erroneous data, but not for their erasure, because even erroneous medical data might have their importance for the data subject's medical history.

164. It is clear that the data subject cannot be enabled to obtain rectification of medical data to which he/she has not been given access - direct or indirect - under Principle 8.2.

165. Personal data in a medical file may be accompanied by "judgmental data": opinions and evaluations made by the persons in charge of the medical analysis or treatment which thus also constitute medical data, but data on which these persons may claim a certain right of determination. Although the drafters of the recommendation recognised that, as in the employment sector (Recommendation No. R (89) 2), the data subject should in principle have the right, in accordance with domestic law, to contest judgmental data in his/her medical file and have such contest recorded, they admitted that to formulate a specific principle on this issue would meet with too many difficulties in practice.

166. Following the preceding Recommendation No. R (81) 1 on regulations for automated medical databanks, the drafters of the recommendation considered that data subjects should be allowed to appeal against a refusal to rectify erroneous data. Depending on domestic law and national practice, such appeals could be lodged either with the competent tribunal, or the data protection authority. If, in accordance with Principle 9.3, the controller of a medical file has drawn up internal regulations, such appeal might be addressed to either the person or body to whom certain decisions must be submitted for approval, or the person who supervises the use of the medical data file, or the person to whom appeal may be made in the event of dispute, if such persons have been designated in the internal regulations (see paragraph 179 hereafter).

Unexpected Findings

167. As indicated in paragraphs 119 and 160 above, unexpected results of a genetic analysis may cause harm to the data subject or other members of the genetic line which is of more importance than the data subject's right to know his/her own genetic data, for example, presence of unexpected family relations, or absence of presumed family relations. Such incidental data were not the purpose of the analysis; nobody asked for them. Moreover, Article 5 of the convention requires that data undergoing automatic processing shall be adequate, relevant and non-excessive. The best protection of such incidental data would be their immediate erasure.

168. Paragraph c of Principle 8.2 allows access to genetic data to be refused, limited or delayed, if it is provided for by law, if revealing these data is likely to cause serious harm to consanguine/uterine kin or to a person in the direct genetic line (see paragraph 160 above).

169. However, the drafters of the recommendation were aware that the convention also requires in Article 8 that the data subject shall be enabled to have access to his/her data. In the genetics sector, the right of access to probably complex data should be understood rather as a right to comprehensible information for the data subject. Moreover, it was noted that Principle 11 of Recommendation No. R (92) 3 on genetic testing and screening for health-care purposes was worded as follows:

"In conformity with national legislation, unexpected findings may be communicated to the person tested only if they are of direct clinical importance to the person or the family.

Communication of unexpected findings to family members of the person tested should only be authorised by national law if the person tested refuses expressly to release information even though the life of the family members is in danger."

170. For these reasons Principle 8.4 does not entirely exclude the possibility that information on unexpected findings be given to the person subjected to an analysis. However, the following conditions must be met:

either

a. domestic law must not prohibit such information; and

b. the person himself/herself has asked for the information; and

c. the information is not likely to cause serious harm to his/her health (physical or mental) or cause harm to certain categories of persons;

or

the information is of direct importance for the treatment of the person or for the prevention of harm to his/her health, or is not prohibited by domestic law.

171. The categories of persons who should not be harmed include, first of all, consanguine/uterine kin, that is members of the genetic line of the person who has undergone the genetic analysis. Secondly, the drafters of the recommendation believed that this protection should also be extended to persons belonging to his/her social family, that is the persons who, while not belonging to his/her natural or legal family, are however linked by ties of affinity, such as the spouse or an adopted child. Thirdly, protection should be extended to those people who are not members of the genetic line or of the social family, but who have a direct link with the person who has undergone the analysis, for example the sperm donor.

172. In certain member states, domestic law does not permit information on unexpected findings to be concealed, in the interests of a third party, from the data subject who has made the request for the information. Principle 8.4 permits, in this case, a derogation from this restriction of information, on condition that domestic law provides other appropriate safeguards to protect third persons.

173. Since Principle 8.4 already constitutes a derogation from the right of access the restrictions set out in Principle 8.2 do not apply to it.

9. Security

174. As a first rule, the general provisions regarding security laid down in the convention apply to medical data files, and in particular its

Article 7. Principle 9.1 takes up this provision, adapts it to the particular nature of medical data and to the special conditions in which they are collected and expands it further.

175. The drafters of the recommendation believed that the measures laid down in Principle 9.1 should also be taken with respect to genetic data and, as far as possible, should cover the carriers of these data, such as samples taken from human bodies.

176. Furthermore, under Article 6 of the convention, personal data concerning health may not be processed automatically unless domestic law provides appropriate safeguards.

177. The drafters of the recommendation underlined the growing importance of security measures, because of the increased use of electronic equipment by general medical practitioners, the many thefts of such equipment and the relatively low expenses incurred by the implementation of such

measures. Therefore, Principle 9.2 requires in particular a policy aimed at ensuring the security and accuracy of medical information systems, including a number of security counter-measures similar to those defined in Article 118 of the convention implementing the Schengen Agreement of 14 June 1985. Such measures should balance the smooth functioning of the system for the benefit of the patient against the safeguards necessary for his/her privacy to be protected against undue intrusion. They should keep up with the technological developments in information systems, without however leading to disproportionate expenses.

Moreover, the measures should be appropriate. For instance, a practitioner should not leave his/her personal computer in an unlocked room; larger health-care centres should be equipped with code systems for access to computers.

178. In respect of sub-paragraph e of Principle 9.2 (access control), the system design should be appropriate to the circumstances, for example, to keep the different types of data together when this would facilitate the patient's care and treatment. Information should preferably be available only on a need-to-know basis.

179. In the case of medical files of a certain volume, to which, apart from the person in charge of medical treatment, other health-care professionals have a legitimate access, Principle 9.3 recommends that the controller of such files draw up, in conformity with domestic law, internal regulations to ensure respect of the relevant principles in this recommendation. Such regulations should also designate the persons with whom an appeal could be lodged if rectification of erroneous data were refused (see paragraph 166 above).

180. Where controllers of medical files cannot themselves ensure that security measures are being respected, they should under Principle 9.4 appoint information security agents, not in order to pass on their own responsibility for the security of the medical data, but in order to delegate some of their tasks.

10. Conservation

181. The recommendation takes account of a situation in which medical data files must be treated differently from most other types of data files. As a general rule, expressed in Principle 10.1, medical data must not be stored longer than is necessary, for it is a threat to his/her privacy if information relating to any individual is allowed to accumulate as the years go by.

182. However, the interests of public health, medical research, the treating physician, the controller of the file or historical or statistical reasons may require the long-term conservation of medical data, even after the death of the persons concerned. Specific regulations exist in a number of member states for the conservation of medical archives. Principle 10.2 permits the long-term conservation of medical data, provided that adequate safety and privacy safeguards are given.

183. Personal data collected during genetic screening and diagnosis and associated genetic counselling may be stored, including data on genetic counselling, diagnosis and prevention of disease. For purposes of medical care - diagnosis, treatment and prevention of disease - and for related research, long-term storage of genetic data may be needed because of the nature of genetic diseases. Particular consideration should be given to specific security requirements necessitated by the long-term storage of genetic data.

184. Principle 10.2 can also apply to incidental data resulting from genetic analysis.

185. When medical data are conserved, the privacy of the patient is best safeguarded by anonymisation of his/her data. If this is not possible, other special safety measures must be taken for this purpose.

186. However, none of these safeguards affects, in principle, the right of the data subject to require erasure of his/her medical data once they are no longer useful for the purpose for which they were collected. This right can be restricted only by overriding and legally protected interests, for example legal obligations to store medical data in archives, or when domestic law does not allow erasure by the data subject, or when the legitimate interests of the health-care professional to conserve data of his/her patients to defend himself/herself against possible allegations of incorrect diagnosis or treatment would oppose erasure (Principle 10.3).

187. The drafters of the recommendation did not include a provision on the transfer of medical data to another health-care professional, if the data subject asked for this, because of the questions which such obligation would raise outside the scope of the recommendation.

11. Transborder data flows

188. With the increasing mobility of persons, the transborder flow of medical data becomes more and more important: the life of the data subject may depend on the rapid and uncomplicated communication of his/her medical data.

189. Yet, with a view to the sensitive nature of medical data and the risk which unauthorised access poses for the data subject's privacy, Principle 11.1 confirms explicitly that the provisions in this recommendation apply also when medical data are transferred across the border. In this, and in the following Principles 11.2, 11.3 and 11.4, the recommendation follows Recommendation No. R (91) 10 on the communication to third parties of personal data held by public bodies.

190. Principle 11.2 sets out the principle of free flow of data. Since a contracting party to the convention must be possessed of data protection norms consistent with the convention's basic principles, there is no prima facie justification for restricting the flow of data to it. This is certainly the case when the exporting state is also a contracting party. However, Principle 11.2 is not exclusively concerned with the situation in which the communicating country is a contracting party. It also envisages personal data being communicated by states not party to the convention, including states which have not yet adopted legislation on data protection. The drafters of the recommendation have sought to encourage the acceptance by all countries of the principle of free flow of data to states which have ratified the convention.

191. The provisions of Principle 11.2 are without prejudice to the right of a contracting party to determine the conditions for the transfer of particular categories of personal data or personal data files in accordance with the provisions of Article 12, paragraph 3.a of the convention.

192. Principle 11.3 deals with the situation in which the state of destination ensures protection of medical data which is in accordance with the basic principles of the convention as well as the philosophy of this recommendation, but has not yet ratified the convention. Certain states have in fact adopted data protection laws in conformity with the convention but have not yet reached the stage of depositing their instrument of ratification. As in Principle 11.2, Principle 11.3 similarly encourages the free flow of data to such states. It is felt that even though ratification of the convention is an absolute necessity at some stage, the legal situation in regard to data protection in such countries should be accepted as sufficient and transborder communication should be allowed to take place without further conditions. To use the terminology of the convention, an "equivalent level

of protection" may be deemed to exist in such countries, at least when the data are to be imported from the territory of contracting parties.

193. Principle 11.4 deals with a situation in which the state of destination has not ratified the convention and does not ensure the effective protection of personal data which can be considered to be compatible with the basic principles of the convention. In this case, and so as not to weaken the protection of data subjects and so undermine the scope of data protection principles, in particular the principles laid down in the convention as well as in this recommendation, exporting states should allow communication of medical data to third parties resident in such countries, only if one of the two conditions hereafter is met.

194. Sub-paragraph a of Principle 11.4 provides for an alternative method of ensuring data protection in the event of communication of medical data to countries which have not yet legislated for data protection. The alternative method envisages the exporting country taking measures which could guarantee the integrity of the data, including respect of the principles laid down in the convention and in this recommendation, in the territory of the country of destination. One such measure could require the importing third party to commit itself contractually to respecting data protection principles. In this regard, reference should be made to the model contract which has been drawn up by the consultative committee of the contracting parties to the convention. The use of contract law, it should be emphasised, is to be regarded as a stop-gap measure pending the enactment of data protection provisions in the country of destination and should not be seen as replacing the need to adopt such provisions at some stage. In order to allow for dispute resolution free from considerations of national law, the contract should provide for a system of independent arbitration. The competence of the independent arbitrators should extend to enabling the data subject to enforce his/her rights in regard to his/her data and to awarding him/her compensation in the event of such rights being denied by the third party. Principle 11.4, sub-paragraph a, stresses that the use of such measures as an alternative to protection by domestic law is conditional on the data subject being informed of the possibility that his/her data may be communicated to third parties situated in countries not having data protection provisions, and being given the opportunity to object to the communication.

195. In the second place, the drafters of the recommendation have suggested that communication could take place if the data subject had given consent, and thereby had taken the responsibility in the circumstances envisaged for his/her medical data to be communicated outside his/her national territory to a country where it is impossible to monitor the fate of the data.

196. Principle 11.5 recommends that in the case of transborder data flows appropriate supplementary measures be taken for the security of the data. The exporter of the data should, in such cases, indicate the purposes for which the data were collected, and the persons to whom they may be communicated. The importer should undertake to respect these purposes, and not to communicate to other persons or bodies, unless he/she is obliged to do so under domestic law (for example in criminal investigations). It is clear that such supplementary measures cannot be required in emergency situations, and are superfluous when the data subject has himself/herself accepted the transfer.

12. Scientific research based on medical data

197. Although the recommendation does not refer to it explicitly, the requirement in Article 5 of the convention that personal data undergoing automatic processing should be adequate, relevant and not excessive applies equally to medical research: only the data necessary for the purposes of such research should be used.

198. The primary means of protecting medical data to be used for scientific research purposes, called for in Principle 12.1, is to make them anonymous. For this reason, researchers as well as public authorities concerned are urged to develop anonymisation techniques.

199. The second means of protection advocated by the recommendation involves arrangements for supervising planned research projects based on the quality requirements laid down in Article 5.b and 5.c of the convention (Principle 12.4; see paragraphs 211-212 hereafter).

200. The nature or objectives of certain research projects sometimes make it impossible to use anonymous data. In such cases under Principle 12.2 personal data may be used if the purposes of the research project are legitimate and one of the conditions listed is fulfilled.

201. Firstly, personal data may be used for medical research if the data subject has been duly informed of the research project - or at least if the information requirements in Chapter 5 have been respected - and has given his/her consent for that particular project, or, at least, for the purposes of medical research (sub-paragraph a).

202. Secondly, in the case of a legally incapacitated person, this consent must have been given in accordance with Principle 6.4, and the research project must have a connection with the medical condition or disease of the data subject (sub-paragraph b).

The drafters of the recommendation agreed that any consent given on behalf of a legally incapacitated person should not be motivated by material interests, but that any explicit requirement along these lines would be outside the direct scope of this recommendation.

203. Thirdly, cases may arise where the data subject cannot be found or where for other reasons it is apparently impossible to obtain consent from the data subject himself/herself (for example, in the case of an epidemic). When in such cases the interests of the research project are such that they justify the consent requirement to be waived - for example in the case of an important public interest - and unless the data subject has explicitly refused any disclosure, then the authorisation to use personal data may be given by the body or bodies designated by domestic law and competent in the area of personal data. The drafters of the recommendation agreed that such authorisation should, however, not be given globally, but case by case; moreover, the medical data should be used only for the medical research project defined by that body, and not for another project of the same nature (sub-paragraph c).

204. The authorisation, by the designated body, of communication of medical data for the purposes of a medical research project also depends on other factors implicit in the spirit of the recommendation in the present principle, or explicitly set out in other principles:

a. the existence of alternative methods for the research envisaged;

b. the relevance of an important public interest of the aim of the research, for example in the field of epidemiology, of drug control or of the clinical evaluation of medicines;

c. the security measures envisaged to protect privacy;

d. the necessity of interfering in the privacy of the data subject.

205. Furthermore, the drafters of the recommendation specified that opposition by the data subject need not necessarily intervene before communication of his/her medical data; he/she could also appeal against the authorisation given by the body concerned, on condition nevertheless that such appeal does not jeopardise the whole research project. The form of this kind of appeal would depend

on the system provided by domestic law (authority responsible for data protection, ethics committee, court, etc.).

206. The drafters of the recommendation agreed that under sub-paragraph c.ii it would not be necessary to make the reasonable efforts in all cases; the person in charge must, however, consider whether with reasonable efforts it would be practicable to contact all data subjects. If this seems possible, then the efforts must be made.

Furthermore, it was understood that to seek the consent of the data subject for medical research would be an unreasonable demand for the research institute, and would rather be the responsibility of the person or body envisaging disclosure of medical data.

207. The expression "disclosure of data" in sub-paragraph c was translated into communication des données in the French version. Whilst accepting that this translation did not reflect in full the English expression, the drafters of the recommendation agreed that the intended meaning of this principle was to subject, in the conditions described, not only any use, but also any transmission of medical data for medical research, to prior authorisation.

208. Finally, medical research may be based on personal data, without the data subject's consent, if the research is provided for by law (not necessarily "explicitly authorised") and constitutes a necessary measure for reasons of public health, including therapeutic research (sub-paragraph d).

Because of the stricter protection of medical data required by Article 6 of the convention, sub-paragraph d, in allowing such exceptions, is less flexible than Article 9 of the convention.

209. As in paragraph 75 above, the drafters of the recommendation noted that under "law", in sub-paragraph d, should be understood any mandatory ruling, whether general or subsidiary legislation, for example a ministerial decree, as long as the ruling is based on domestic law and is sufficiently accessible and foreseeable (see the case-law of the European Court of Human Rights).

210. Principle 12.3 recognises that medical doctors and medical bodies entitled to carry out their own research should be allowed to use, for their own research, the medical data which they have collected themselves, if the data subjects are aware of such use and have not objected, that is, they had been informed that one of the purposes of the collection would be medical research. These complementary provisions may in particular consist of the consent of the data subject or of permission given under domestic law or by a controlling body for public health reasons.

211. Medical research using personal data may raise problems connected with data protection, which are addressed in this recommendation, but also incidental questions of an ethical and scientific nature, such as:

a. the need for research involving personal data;

b. the suitability of the data to be collected for a particular research project;

c. the exhaustive nature of the research project;

d. the processing of the data of the unborn and deceased;

e. the information of the patient and his/her family;

f. the ways and means of collecting the data;

g. the communication of the research findings.

212. Depending on domestic law, these questions may have to be solved, preferably in advance, by one or more specific bodies designated by law and responsible for the questions within their sphere

of competence. The drafters of the recommendation considered that it would be outside the scope of the recommendation to address such ethical and scientific questions raised by medical research, or to designate the bodies responsible for solving such questions. They referred to national legislation, which in the case of various bodies should distribute responsibilities and ensure co-ordination.

Principle 12.4 requires therefore merely that any such ethical and scientific questions be examined, apart from the data protection point of view, also in the light of other relevant instruments in the field of ethics or science.

213. By "exhaustive nature of the research project" in sub-paragraph c of the preceding paragraph, the drafters of the recommendation had in mind a project requiring the collection of medical data concerning all persons affected by such research, with or without their consent. The effectiveness of certain types of epidemiological research in fact depends on the recording of data concerning all the patients infected.

214. The general principle of purpose specification applies in particular to the processing of personal data for medical research: such data collected, processed or disclosed for one specific project should not be used for another project, or for purposes other than those for which the consent or the authorisation has been given under Principle 12.2. If the second research project, for which the data were not collected, or for which consent or authorisation was not given, is substantially different from the first project, then the whole procedure defined in Chapter 12 should be followed again.

215. Although it may seem obvious that the possibility to use personal data in medical research does not imply that the results of the research may be published in a form which enables identification of the data subjects, the drafters of the recommendation thought it wise, because of the sensitive nature of medical data, to emphasise this requirement in Principle 12.5. In some member states, publication of medical data is, however, prohibited, even if the data subject has consented.

Footnotes

1. Hereafter referred to as "the convention".

2. Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector; Resolution (74) 29 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector.

3. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Strasbourg, 28 January 1981, ETS No. 108). At the time of publication of this explanatory memorandum, seventeen states had ratified the convention: Austria, Belgium, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Luxembourg, Netherlands, Norway, Portugal, Slovenia, Spain, Sweden and United Kingdom.

4. Albania, Andorra, Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Moldova, Netherlands, Norway, Poland, Portugal, Romania, Russian Federation, San Marino, Slovak Republic, Slovenia, Spain, Sweden, Switzerland, "the former Yugoslav Republic of Macedonia", Turkey, Ukraine and United Kingdom.