AUTOMATION, PRIVACY PROTECTION AND THE LAW

J.K.M. Gevers

Introduction

This paper deals with the legal aspects of privacy protection in relation to the introduction of automated information systems. In itself, the process of automation gives rise to several other legal problems, in addition to issues in the domain of privacy and confidentiality; the question of potential negligence or liability arising from the use of defective computer software is an example. On the other hand, also the concept of privacy protection is much broader than only the issue of data protection; in the European Convention for the Protection of Human Rights, for instance, the right to privacy is defined as everyone's right to his private and family life, his name and his correspondence. In the following however, I will limit myself to the specific legal issues relating to the storage of medical data in computerised information systems or data banks.

Generally the automation of existing health information systems provokes concerns about data protection. These concerns can be explained partly by the fact that medical data are regarded as particularly sensitive. However, also several features characteristic of automated systems play a role: automation makes it possible to maintain and to handle very extensive record systems; data are easily available and can be transfered quickly from one information system to another; moreover, data can be combined in ways which might not otherwise be practicable [1]. Nevertheless, it would be a mistake to suppose that the problem of data protection is exclusively related to automation. Also conventional methods of storing medical data give rise to problems of data security and confidentiality. The process of automation, however, has given the older problems new dimensions and added new problems. Still, it is remarkable that the legal instruments relating to privacy protection which have been developed over the last ten years both at national and at international level, are very often only directed to automated information systems.

Before giving a brief survey of the data protection principles, in particular as laid down in international documents, I will say a few words about the relationship between the more encompassing concept of privacy and the traditional concept of professional secrecy. Subsequently, attention will be paid to the emerging principles of data protection, using the Council of Europe's Recommendation on Automated Medical Data Banks as an

C. Th. Smit Sibinga et al. (eds.), *Automation in blood transfusion*

example. Finally, I will venture into a field which is much more familiar to most of you than to me, and try to delineate some implications for blood banks.

Medical secrecy and privacy protection

The confidentiality of data relating to identifiable patients or clients has always been a basic principle in health care. For a long time however, confidentiality of patient records was mainly considered as a problem of medical ethics. Professional secrecy was seen as inherent in the fiduciary relationship between the patient and his doctor. The predominant issue was in which exceptional circumstances the individual medical professional would be justified in disclosing information about his patient to third parties. These traditional understandings of confidentiality, expressed in the obligation of professional secrecy, are no longer sufficient to deal with the confidentiality issues raised by a modern health care system.

First of all, the traditional tenets of confidentiality are effected by the fact that in the health care system of today medical data are collected, stored and used on a very large scale and for a variety of different purposes. Although the disclosure of these data to third parties has reamined an important issue, new problems arise from the mere collection, processing and keeping of information. Secondly, to a growing extent medical data are kept by organizations and institutions instead of individual health professionals. Examples may not only be found in the modern hospital where there is a wide circle of professional and technical staff which generate and handle the data stored in the centralised information system, but also in other domains, e.g. in preventive care, where medical data, even if originally collected by an individual practitioner are often under factual control of a service or an agency. This process has been facilitated by the computer, which has changed many health care professionals from custodian of patient records into users of data systems controlled by large institutions.

These developments have not made the traditional philosophy of professional secrecy irrelevant; actually the core of the classical doctrine, i.e. the principle that a doctor should not divulge what he sees or hears in the course of his profession, is as relevant as ever. The point is, that this principle alone is not sufficient, basically because it is directed to individual professionals (and not to organizations and agencies) and because it focuses on disclosure (and does not pay due attention to collection, storage and keeping of data). It is with a view to this situation, that the more encompassing concept of informational privacy has developed and is being applied to medical data. Privacy protection does not stand for one single set of rules.

Given the tremendously varied and complex issues of citizen rights in health record keeping there is no hope that one single law could provide the answer [2]. Rather, privacy is a broad objective. Elaboration of standards, applicable to the widely varying situations where it is at stake, is only feasible at the abstract level of very general directives, which have to be

worked out into more detail at a much lower level; very often this will be the level of the organization which maintains the information system.

General directives

In the recent past, many industrialised countries have adopted privacy legislation relating to automated data systems. To give a brief account of the general principles embodied in such legislation it is useful to look at the international legal documents on the same subject matter. In Europe, it is the Council of Europe which has been very active in this field. In addition to its Recommendation on Automated Medical Data Banks, it has elaborated a Convention on the protection of individuals with regard to automatic processing of personal data. This convention was adopted in 1981, and has now been ratified by many countries. The countries which have become party to the treaty are obliged to give effect to the basic principles laid down in it in their domestic law. Basically, these principles amount to the following.

Personal data undergoing automatic processing must be obtained fairly and lawfully. They must be stored for specified and legitimate purposes and not used in a way incompatible with those purposes; they must be adequate, relevant and not excessive in relation to the purpose for which they are stored and they should be preserved in a form which permits identification of the data subjects for no longer than is necessary. Furthermore, appropriate security measures must be taken for the protection of data against accidental or unauthorised access, alteration, destruction or dissemination. Finally, any person must be enabled to establish the existence of an automated personal data file, to obtain confirmation of whether data relating to him are stored in it as well as communication to him of such data in an intelligible form and to obtain rectification or elimination of these data if they are incorrect or irrelevant. Particular mention should be made of art. 6 of the Convention which prohibits the automatic processing of personal data concerning health unless domestic law provides appropriate safeguards.

To know what safeguards are considered appropriate by the Council of Europe we have to look at the Recommendation on Automated Medical Data Banks, which was adopted by its Committee of Ministers in the same year as the Convention [3]. The most important element in the Recommendation is, that every medical data bank must be subject to its own specific regulations, in conformity with the laws of the state in whose territory it is established. These regulations should be sufficiently specific to provide ready answers to those questions likely to arise in the operation of the particular data bank. Particular reference is made to the regulations of data banks used for purposes of public health, management of health services or the advancement of science: such regulations should have due regard to the preeminence of individual rights and freedoms. Apparently, the Council of Europe was concerned that especially in these types of data banks individual rights would easily be compromised.

The Recommendation then goes on to state which provisions a data bank's regulations must contain. Mention is made, sub alia, of the data bank specific purposes, the categories of information recorded, the security and conservation of data, and the organization for whom the data bank is operated and who supervises the use of the data bank. Provisions must also be elaborated on the categories of persons who are entitled to cause data to be placed in storage, modified or eliminated, as well as on the persons who have access to the data bank in the course of their work and the categories of data to which they are entitled to have access. As a general rule access to the information may be given only to medical staff and, as far as national law or practice permits, to other staff, each person having access to those data which he needs for his specific duties. If appropriate, records must be so designed as to enable the separation of data relating to the identity of persons, administrative data and medical data.

Two items of particular importance on which a data bank's regulations must contain provisions, are the disclosure of information to the data subjects themselves and the disclosure to third parties. An individual must always have access to his own record: every person has the right to know the content of the information held about him in a medical data bank, thus the Recommendation. However, the national law may provide that this information may be communicated to the data subject through the intermediary of his physician. As far as disclosure to third parties is concerned, the Recommendation refers to the rules of medical professional secrecy which require the data subject's express and informed consent, in particular if medical data are communicated to persons or bodies outside the field of medical care.

The effect of the Recommendation of the Council of Europe depends of course on the extent to which individual countries adopt legislation to make the aforementioned safeguards operational. In the Netherlands, we are still in the process of developing statutory safeguards for medical information systems. One set of rules has almost been completed now; it is a general privacy protection act (Wet Persoonsregistraties), which provides sub alia an obligation to elaborate specific regulations for automated information systems in the health care sector. Another set of rules, dealing with patient rights has only appeared in the form of a first draft; in addition to rules on informed consent, it also contains rules on privacy protection, including professional secrecy, access to records, the conservation of records and the right to have recorded data erased from the record. Both sets of rules apply also to blood banks.

Implications for blood banks

This leads us to the implications of these general privacy standards for blood banks. Blood banks will collect and store many and sometimes particular sensitive medical data on donors. Therefore, the privacy protection standards mentioned before are directly applicable to blood banks. Blood banks

have specific reasons to respect these standards. First, they have a legal duty to protect the physical and moral integrity of the donor, as is apparent from many national laws on blood transfusion. Secondly, any doubt on privacy protection safeguards might deter potential donors from volunteering to donate blood.

If automated information systems are introduced, blood banks should adopt in accordance with national law regulations concerning the ways personal data are processed. The function of such regulations is not only to give internal guidance, but also to inform donors on how the system operates and what their rights as data subjects are. Of course such regulations need not to be elaborated by each individual blood bank on its own; another possibility is development of model regulations that can be adopted by more than one blood bank. Basically such regulations should contain provisions on the different aspects of automatic processing of personal data.

I have already mentioned the most important of these aspects. Some of them deserve further attention in connection with blood transfusion services, i.e. access to stored donor data and disclosure of such data to third parties.

The extent to which confidentiality of donor data can be safeguarded depends to a considerable degree on the arrangements concerning access to the system and the measures to prevent unauthorised access. In this point legal documents very often give little guidance. Under the Dutch privacy act, for example, blood banks maintaining an automated information system are only under a general obligation to do what is necessary with respect to data security and to see to it, that each person working in the organization can only have access to what he needs for his work. The law does not say which technical and organisational measures are feasible and appropriate to ensure that no unauthorised access takes place. Instead, it leaves much discretion at blood banks to adopt the solutions they consider adequate. Blood banks, with their strong commitment to protection of the donor, should place a high value on privacy protection and adopt all measures which are reasonably possible also if they entail organisational or financial burdens.

The privacy of the donor is directly at stake when personal data are conveyed to third parties. As far as disclosure to third parties is concerned, blood banks have to comply with the traditional rules relating to the strict confidentiality of medical data. Unless national law provides for an exception, the express and informed consent of the data subject is required for any communication of his personal data to others. In my opinion this also means, that the results of medical examinations or of screening of donor blood should not be communicated to his general practitioner without the donor's express consent. One could object, that normally in curative care the patient's permission to sharing of information between his doctor and other staff involved with his treatment, is presumed. Such a supposition would not seem justified in this situation, however; here, there is no request of the patient for help; moreover the patient may have a strong interest in certain data (e.g. concerning sexually transmitted diseases) not being com-

municated to his general practitioner [4].

If potential donors do not pass medical examination or screening, they are placed on a deferral list. Reasons for donor deferral may relate to very sensitive information. Here it is essential, that blood banks do not enter more data into the system than is absolutely necessary. It goes without saying that information on the reasons for deferral should not be shared between blood banks without the donor's consent. The same would seem to hold for the mere fact that a donor is rejected.

Blood banks may come under strong pressure to disclose information about a donor in a case of post-transfusion infection. Also in such an event confidentiality prevails, which means that blood banks must refrain from providing data which can be related to an identifiable donor or from disclosing the identity of the donor of a particular unit of blood.

How strong the pressures on blood banks sometimes can be, is exemplified by a case decided by the Florida Supreme Court in 1987. After a traffic accident, a patient was given 51 units of blood during emergency treatment; a year later he was diagnosed as having AIDS. After the patient died in 1984 the family tried to find out, whether one of the donors involved was contaminated with the AIDS-virus in order to sue him for damages. However, the supplier of the blood refused to disclose the identity of the donors to the lawyers of the family. A lower court decided, that the blood service did not have to provide a list of the donors, since their constitutional right to privacy would be violated if such a list was released [5]. The Florida Supreme Court confirmed this decision; it recognised the plaintiff's interest, but it reasoned that this interest was overriden by the privacy interests of blood donors and the public's interest in maintaining a strong volunteer donation system [6].

This case may seem an exceptional one and probably it is, at least in countries with a system of compensation for personal injury and death different from that in the U.S. Yet the case is interesting because the court decisions in which it resulted underline very well that confidentiality surrounding blood donations is not only required by every citizen's right to privacy, but is also a cornerstone in a system of voluntary blood donation.

References

1. Vuori H. Privacy, confidentiality and automated health information systems. J Med Ethics 1977;3:175-8.
2. Westin AF. Patient's rights: Computers and health records. Hosp Progr 1977;58:60
3. Council of Europe. Recommendation No. R(81)1 on regulations for automated medical data banks, adopted by the Committee of Ministers on 23 January 1981. Int Dig of Health Legislation 1981;32:740-4.
4. Leenen HJJ. Legal aspects of the use of information systems in health care. In: Fokkens O (ed). Medinfo - 83 Seminars, IFIP-IMIA North Holland 1983:51-4

5. Birchfield JL. AIDS: The legal aspects of a disease. Med and Law 1987;6:407-26.
6. Gostin LO, Curran WJ, Clark ME. The case against compulsory casefinding in controlling AIDS-testing, screening and reporting. Am J Law and Med 1987;12:7-53.