Protection of personal health information in the Netherlands: getting the balance right?

J C J Dute

Introduction

Health records are important not only as part of the process of providing care but also for wider purposes such as quality control, research, and service planning. In principle, personal health information has to be kept confidential. In the Netherlands the obligation of the healthcare provider to safeguard confidentiality derives from criminal law, administrative law, and contract law. A healthcare provider also risks disciplinary action when violating confidentiality.

The legal rules concerning the protection of health data in the Netherlands are laid down in detail in the Data Protection Act, which covers all personal information held on computer or otherwise systematically stored, and in the Medical Contract Act. That act provides for specific rules on the healthcare sector, in addition to the protection offered by the Data Protection Act. The patient's right to privacy is furthermore supported by the Dutch Constitution (article 10) and several international treaties – for instance, the European Convention for the Protection of Human Rights and Fundamental Freedoms (article 8).

The Medical Contract Act came into force on 1 April 1995. It regulates in general the contractual relationship between patient and healthcare provider. As a result, a catalogue of patients' rights is inserted in the Civil Code. Specific rules are laid down concerning the disclosure of information for research and preparing the use of coded data. From this legislation the question arises whether a fair balance has been struck between the patient's interests concerning privacy and the needs of quality control and scientific research. This article gives a brief overview of the legal rules for the protection of personal health information in the Netherlands and discusses the implications of this legislation for quality control committees and researchers.

Personal health information

According to the Data Protection Act, personal information is information that can be linked to an identifiable individual. Simply anonymising the data does not guarantee that the identity of the patient will not or cannot be disclosed. Distinguishing features have to be removed in such a way that it will require a disproportionate amount of time, money, and resources to link the anonymised data to the patient from whom it was derived. Whether or not this – rather stringent – criterion is fulfilled depends on, among other things, the nature of the information and the technical facilities of the

recipient. Once information is unidentifiable it is beyond the reach of privacy laws.

The fulfilment of this criterion poses serious problems for researchers who want to make use of coded data without the consent of the patient, because a code does not prevent the identity of the patient being disclosed in all circumstances. Sometimes additional information or prior knowledge enable the coded information to be linked to an individual. For example, coded information about a 24 year old male butcher with tuberculosis living in the small village X has to be considered as personal information because it will be easy to identify the person the information applies to. As we shall see later, this problem has been tackled in the Medical Contract Act.

Collecting and storing personal health information

The Data Protection Act allows personal data to be collected only when necessary for the proper fulfilment of the task imposed on the record keeper. Furthermore, only those data may be recorded that are necessary for the specific purpose of the data collection (the so called double necessity criterion). Only lawfully acquired data may be stored. For every data collection rules explaining the way in which the system operates have to be drawn up by the record keeper (self regulation).

According to the Medical Contract Act, the healthcare provider is obliged to record the necessary information on the treatment of the patient. These records have to be kept for 10 years. They may be kept for a longer period when required by "good physicianship".

Patients have the right of access to their own records. The right of access to health records has been recognised before in jurisprudence and in the Data Protection Act. In the Medical Contract Act it has been sharpened: access can be denied only if vital for the protection of the privacy of others. Patients are entitled to add comments to their health records and to ask the healthcare provider to correct inaccurate, incomplete, or irrelevant information. Health data have to be deleted on request of the patient, except in the case this would prejudice substantial interests of others (including the healthcare provider) or would cause a violation of the law.

Disclosure of personal health information

Disclosure of personal health information to others than the patient is allowed only with the consent of the patient, when required by law or in case of conflicting interests.

University of Limburg,
Department of Health
Law, PO Box 616,
NL-6200 MD
Maastricht,
Netherlands
J C J Dute, associate
professor of health law

Accepted for publication
13 June 1995

Oral consent by the patient is sufficient. No express consent has to be obtained when the information is passed on to those who are directly concerned with the patient's care, provided that only such information is disclosed that is needed to perform their duties. Parents and guardians may under certain circumstances be informed without the patient's express consent unless this would run counter to "good physicianship."

There are only a few examples laid down in law in which disclosure of confidential information is required. The Act on Infectious Diseases Control, for instance, imposes a duty on the physician to notify cases of certain infectious diseases to the director of the municipal health service. Another example is the physician's obligation to procure the registration officer data on the birth of a child.

A conflict of interests may arise when vital interests (for example, life or health) of other individuals are threatened and the problem can be solved only by violating professional secrecy – for instance, in the case of (suspected) child-abuse or premeditated murder. The examples illustrate that this justification is limited to rather exceptional cases. Research, planning of healthcare facilities, and similar purposes will not amount to such a conflict of interests.

Disclosure of personal health information for quality control

The Medical Contract Act does not contain specific provisions relating to disclosure of information for quality control. Considering the importance of this subject for everyday practice, this is certainly a weak point in the law.

Although not entirely beyond dispute, it can nevertheless be taken for granted that disclosure of personal information to internal hospital committees for quality control purposes does not require the express consent of the patient. Clinical audit is directly connected with the patient's care and treatment and for that reason disclosure is generally assumed to be implicitly authorised, provided that the information is kept confidential within the review committee and will not be used for criminal or disciplinary actions. The same is true for disclosure of information to hospital committees for reporting accidents and near-accidents.

Disclosure of information to internal review committees in anonymised or coded form is preferable to information that can be linked to an identifiable patient. However, in practice this is not always feasible. Quality review by external bodies using identifiable information always requires the patient's expressly given consent.

Disclosure of personal health information for research

As a rule, disclosure of personal health information for research requires the patient's consent – with two exceptions for research projects in public health.

Firstly, no consent has to be obtained when to ask for this permission is not feasible and the

research project is carried out in such a way that the patient's privacy is not unduly harmed – for instance, when the addresses of the research population can no longer be traced, the patient has died, or asking for consent probably would cause psychological harm.

Secondly, no consent is required when this is not logical considering the nature and purpose of the research project, and data are disclosed to the researcher in such a way that the information cannot reasonably be linked to an identifiable individual. This rule enables the use of coded data without consent. The rationale is that to code information does not protect the identity of the patient in all circumstances. Without a statutory basis even the disclosure of coded information would sometimes require the consent of the patient. This exception was introduced just before the end of the parliamentary discussion on the Medical Contract Act. It is the satisfying result of a sometimes heated debate between lawyers and researchers.

Disclosure in the two cases mentioned above is permitted only when the following conditions are fulfilled: the research project serves general interest; it cannot be carried out without the information to be disclosed; and, most importantly, the patient has not raised objections to disclosure. Furthermore, disclosure has to be recorded in the patient's file. It should be noted that a healthcare provider does not have any obligation to pass on information for research projects. A code of conduct adopted by professional groups of researchers will be issued elaborating the legal provisions on disclosure and use of personal information for scientific purposes.

Discussion

In the Netherlands a fairly strict view is held on professional confidentiality. Personal health information may be disclosed with the patient's consent, by virtue of law, and in the case of a conflict of interests. In this way the Medical Contract Act confirms a long tradition of medical secrecy as a prerequisite for accessible health care.

For the wellbeing of the patient, however, it is necessary not only to protect his or her rights but also to monitor and improve the quality of medical care. The question arises how to strike the best balance between these competing interests. It should be pointed out that, in principle, no personal information should be disclosed without the consent of the patient, for quality control or for research. However, when obtaining consent constitutes a major obstacle in performing these essential tasks, involving the risk of neglect, the legislator should not hesitate to interfere. Such legal rules should leave the right to self-determination of the patient as unaffected as possible.

In any case the use of anonymised (if necessary coded) data is preferred unless the recipient needs to know the identity of the patient. For internal quality control, however, disclosure of personal information can be justified on the basis of implied consent, provided the

patient is properly informed. This should be laid down by law accompanied with rules safeguarding confidentiality within the internal review committees. In this respect the Medical Care Act leaves room for improvement. Of course, the question remains as to what extent the patient is free to object to disclosure, especially when certain information is absolutely necessary for quality control.

In my opinion the use of coded information strikes a fair balance between the right to privacy and legitimate research interests. Replacing the patient's consent by a right to object accompanied by a high degree of protection of confidentiality offers a great opportunity for researchers who want to exercise due caution. What really matters now is that coding of information becomes everyday practice in research. Furthermore, coding systems should be developed that are practicable and cannot be cracked.

It is very important that patients are adequately informed, in general terms, on the use of information for purposes other than care and treatment, and on their right to object to such disclosures. Here also the right balance has to be achieved since the patient must not be overloaded with information. Special attention has to be paid to the circumstances under which information collected for one research project may be used for the benefit of another. When in doubt about the privacy aspects of a certain research project it is advisable to present the protocol to a special review committee as is the case with biomedical research projects involving human subjects.

In the light of this article, readers are invited to comment in the journal about protection and personal health information in their own countries. Please send contributions for consideration for publication to the Editor.