22

Medico legal issues

GERALDINE MACKENZIE

This chapter aims to provide the reader with an awareness of the legal issues involved in health informatics, an understanding of the need for the privacy and security of the patient record and the legal consequences of a breach of the security of the patient record. The concept of privacy law is introduced and what precautions ought to be taken to minimize legal liability for a breach of privacy and/or confidentiality is discussed.

It may be obvious that there is a need for privacy and confidentiality of the patient record, but the legal implications of a breach of either of these are not always considered and understood. Medical records are by their very nature intensely personal, and a patient must be able to have complete trust in the privacy and security of this information in order to provide it with confidence. Breaches can lead to serious consequences for a patient.

Because of a computer's increased capacity for storage, its enhanced ability to retrieve information quickly and the potential to network large numbers of computers, it is possible for a large number of people to have access to the patient record. Not only is there the possibility that this will result in the leakage of sensitive information, there is also the possibility that electronic records could be altered by unauthorised persons. Although this is also the case with paper records, the potential for harm is not so great.

This chapter examines some legal issues in health informatics; in particular the privacy and confidentiality issues in the electronic storage of health records.

The right to privacy

It is probably fair to say that members of the general public would be of the opinion that they had a right to privacy of their confidential health records. In general ethical terms, they do, but legally it is another matter. The "right to privacy" is somewhat of a misnomer. Generally speaking, there is no such thing as a legal right to privacy in Australia. There has been limited recognition of such a right in, for example, the *Privacy Act* 1988 (Cth) which establishes rights in certain circumstances (see below).

Most breaches of privacy will also be breaches of confidentiality, for which there are other remedies available (see below). The *Privacy Act* was passed by the Commonwealth Government in response to the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. It applies only to "agencies" which are established under

the Commonwealth, and therefore applies only to bodies such as Commonwealth hospitals, the Health Insurance Commission, and the like.

Central to the Act are the 11 Information Privacy Principles which are contained in section 14. They specify such things as the reasons for which information can be collected, how the information shall be stored, how access can be gained to the records, the use to which the records can be put, and the limits on disclosure of personal information. Principle 11 which is particularly relevant, states:

> A record-keeper who has possession or control of a record that contains personal information shall not disclose the information to a person, body or agency, (other than the individual concerned) unless...

A number of grounds upon which the information may be released are then stated, including: (b) the individual concerned has consented to the disclosure.

The Act creates the office of Privacy Commissioner (s 19), who has the power to investigate complaints under the Act. If the Commissioner finds that a complaint is made out, he or she has the power to make various orders, including an order that the complainant be compensated for any loss or damage suffered.

There have been concerns expressed that the Act is not broad enough in its jurisdiction, and also that it may no longer be appropriate to cover computerized record keeping. (O'Connor 1994). There is a need for some sort of legislation to cover medical records more generally, ie, records held by State bodies and private bodies, rather than just Commonwealth agencies as is the case under the *Privacy Act*.

Further to the *Privacy Act*, it is also an offence under s 70 *Crimes Act* 1914 (Cth) for a Commonwealth Officer to disclose information they had a duty not to disclose.

So far, the only State to attempt similar legislation is New South Wales, which has a Data Protection Bill presently before the Parliament, and, when passed, will be similar in content to the Commonwealth Privacy Act.

The duty of confidence

Breach of confidence in a minor matter concerning a patient may be bad enough, but when the breach, for example, reveals that the patient has HIV/AIDS, the consequences for that person can be catastrophic.

A duty of confidence can arise in a number of different ways. It can arise by virtue of the ethics of a profession for example, the AMA Code of Ethics, which states:

In general, keep in confidence information derived from your patient, or from a colleague regarding your patient, and divulge it only with the patient's permission, except where a court demands.

There are also guidelines set down by the various health departments.[i] These type of guidelines can sometimes have a quasi-legal effect, as the courts have examined them when determining whether a duty of confidentiality exists.[ii] There are also statutes in the different jurisdictions which create obligations for confidentiality of health records.[iii]

Furthermore, a duty to keep personal patient information confidential may be an express or implied term of a contract which a patient may enter into with a health provider.

The law also imposes duties in other situations where there is an obligation of confidence arising from the circumstances in which the information was obtained. In order to succeed in this type of legal action, the plaintiff (i.e., the person taking the action), must show that the information must has the necessary quality of confidence about it in the sense that the preservation of its confidentiality or secrecy is of substantial concern to the person taking the court action.[iv] This would almost certainly be the case in a doctor - patient relationship, and other health professional - patient relationships. The second element is that the information must have been imparted in circumstances importing an obligation of confidence; and thirdly that there must be an unauthorised use of that information to the detriment of the party communicating it.[v]

Negligence

Depending on the nature of the breach, the patient may be able to take other legal action against the person responsible. This may be for example, because of the negligence of the record holder in releasing confidential information. Taking such an action can be very difficult, take a long time, and be very expensive. This can be a deterrent in a lot of cases.

According to the law of negligence, a health provider would be liable if he or she owed a duty of care to a patient, that the duty of care was breached by the health provider, and that damage resulted which was causally linked and not too remote. As part of this test, the health provider would be liable if he or she failed to take the necessary steps to eliminate reasonably foreseeable and significant risks of injury to the plaintiff (Trindade & Cane 1993).

Avoiding legal action

The key to avoiding legal action, both for the sake of the patient, and in order to avoid being sued, is to ensure that proper precautions have been taken. This will include putting in place, such things as: proper procedures for record keeping; adequate staff training on an ongoing basis; close and regular monitoring of these procedures, including adequate staff supervision; and review of these procedures making sure that they are sufficient.

Taking these precautions will minimise the exposure to liability for the health professional. It is probably impossible to completely eliminate the risk.

What security measures are needed?

The question of what security measures have to be put in place to safeguard patient records is a difficult one to answer. At the time of writing, there are no standards which apply generally to give guidance in this matter (see further discussion on standards below).

Implicit in this is the need to not only provide an appropriate level to cover all known risks, but also to have a level of security which is sufficient to minimize the risk of legal action.

What precautions must be taken depend on the concept of foreseeability of the breach. The courts have held that even though the risk may be unlikely to occur, it should still have been foreseen, provided that it is not far-fetched or fanciful[vi].

This means that a record holder must take all reasonable steps to safeguard the security of the information. This involves taking proper security measures, such as password protection and not leaving files open on the screen when there is the possibility of access to them by unauthorised persons.

If a record holder takes all reasonable steps to provide proper security, and a breach of security still happens through an event which could not possibly have been foreseen, the record holder would probably not be negligent. This could be contrasted with the position where the record holder has not taken proper precautions, eg staff have not been properly trained, and a breach of security occurs. In these circumstances, the record holder probably would be negligent. Whether or not the record holder actually is negligent is a question which has to be answered in every case. The above examples are a guide only.

Medical records held in networked computers are particularly vulnerable. The potential for outside interference, e.g., by hackers, is real, and must be taken into account. It would be prudent therefore to seek advice from an appropriate computing professional in order to determine the security measures necessary. It must also not be forgotten that these will be subject to change as time passes, due to the changing nature of the computing industry. What is adequate protection today may not be so in one year's time, and almost certainly will not be adequate in five years' time.

If no alterations are made to computer security measures to take account of the changes in information technology and changes in known risks, a person who has suffered harm by the release of the confidential information would have a far greater chance of establishing negligence than would otherwise be the case.

Standards for the keeping of medical records

Although at this time there are no standards which apply generally, these issues are being addressed by a number of bodies. For example, the Royal Australian College of General Practitioners have an *Interim Code of Practice for Computerised Medical Records in General Practice* which was adopted in February 1993 and is to be piloted over two years. The limitation of this Code is that it does not cover all general practitioners, as not all are members of the RACGP.

Standards Australia have in mid 1994 released the *Draft Australian Standard on Information Security and Personal Privacy Protection in Healthcare Information Systems* for public comment. The intention is that the Standard would be adopted by various organisations, who will use it as a base for their own standards.

Although the implementation of standards such as these is to be applauded, record holders adopting them are not automatically guaranteed immunity from legal action. There is still a need to be vigilant, and to note that information technology changes at such a rapid pace, that what is an appropriate standard now may not be so in the future. On the other hand,

a failure to comply with these sorts of standards would leave a record holder vulnerable to legal claims should a breach of security occur.

When can confidential information be disclosed?

There are exceptions to the rule that patient information must be kept confidential, and mandatory HIV/AIDS reporting is one of these. There are other times when access to the patient record is sought, e.g., for medical research, raising both ethical and legal issues. This has been discussed in a recent article (Thomson 1993). In that article, he points out that disclosure of information in medical records for medical research without consent involves a breach of the duty of confidentiality. He then notes three exceptions to the general rule that confidential information cannot be disclosed: (1) where the patient has consented to the disclosure; (2) compulsion of law, where e.g., there is a compulsion to disclose information as part of judicial proceedings, or the mandatory reporting example given above; and (3) where the disclosure would be in the public interest.

An example of the third category occurred in the UK in the case of *X v Y*[vii]. In that case information was supplied to a newspaper that two doctors were carrying on general practice despite having contracted AIDS. One of the issues in the case was whether it was in the public interest that the information be published. The court held that the public interest in preserving the confidentiality of medical records in identifying AIDS sufferers outweighed the public interest in publishing the information, and that this was necessary so that victims would not be deterred from seeking treatment.

A court in the United States has held that in certain situations there is a duty to disclose confidential information in order to warn others who may otherwise be at risk[viii]. This has not yet been followed in Australia although it is possible, (but unlikely) that it could be adopted here one day.

Access to information

Contrasting with the situation previously where patients had limited (if any) access to their medical records, there is now much greater access available with the advent of Freedom of Information (FOI) legislation, although the record is still owned by the person who created it.

Freedom of Information Acts are now present in nearly every Australian jurisdiction except the Northern Territory[ix]. They operate to allow access to information held by certain specified bodies. In most instances, this does not apply to private bodies, like private hospitals, or medical practitioners in private practice. In some jurisdictions, there is no need to rely on procedures under Freedom of Information legislation, as administrative access to records is possible. For example, the Queensland Health Department in 1994 issued their revised policy *Administrative Access to Health Records*. This allows patients access free of charge to their medical records held by Queensland hospitals.

Conclusion

The electronic storage of patient records is increasing in popularity, and before long will be commonplace. It needs to be acknowledged that this brings additional problems of privacy

and security of the information stored in those records. With these problems comes the threat of legal liability to the record holder if confidentiality is breached.

The only way to minimize legal liability and comply with duties of confidentiality is to be aware of the issues, and put in place appropriate mechanisms to address them. It will be necessary in doing this to seek advice from computing / data protection professionals, and where appropriate, take precautionary legal advice. Not only should the legal issues be considered, but also the ethical and moral issues, because the information contained in the patient record is extremely sensitive and it is clearly the obligation of the record holder to safeguard that information. Only then will the health profession continue to maintain the confidence of the public that it presently enjoys.

Book references

Trindade F & Cane P 1993, *The law of torts in Australia*, 2nd ed. Oxford University Press, Melbourne

Journal references

O'Connor K 1994 Emerging information privacy issues in health care. *Proceedings of the Second National Health Informatics Conference* Melbourne, Australia: Health Informatics Society of Australia 21-25

Thomson C J H 1993 Records, research and access: what interests should outweigh privacy and confidentiality? Some Australian answers. Journal of Law and Medicine 1:95-108

Notes

i. See Health Commission of NSW Circulars No 82/369 and 84/82; Department of Health NSW (Hunter) Policy for the Management of Acquired Immune Deficiency Syndrome and Hepatitis B, 1 July 1988; NSW Health Dept Infection Control Policy for HIV, AIDS, and Associated Conditions 1992, Queensland Privacy Guidelines for Hospitals, Department Standing Committee on Privacy and Health and Medical Records, April 1986; WA Health Department Guidelines for Release/Access to Health Records 1986; SA Health Department Guidelines Regarding the Release of Information.

ii. See the case of W. v. Egdell [1990] 1 Ch 359 where the UK Court of Appeal relied on the General Medical Council's Advice on standards of professional conduct and of medical ethics when determining whether a doctor had breached his duty of confidence.

iii. See Health Act 1937 (Qld) s.49(1), Health Services Act 1991 (Qld) s.5.1, Public Health Act 1991 (NSW), Health Administration Act 1982 (NSW), Public and Environmental Health Act 1987 (SA) s.42, South Australian Health Commission Act 1976 s.64, Public Health Act 1962 (Tas), Health Act 1958 (Vic), Health Services Act 1988 (Vic) s.141, Health Act 1911 (WA) s.314, Health Services Act 1990 (ACT), Health Services (Consequential Provisions) Act 1990 (ACT), Notifiable Diseases Act 1981 (NT).

iv. Moorgate Tobacco Co. Limited v Philip Morris Limited (1984) 156 CLR 414, at p 438.

v. Coco v A.N. Clark (Engineers) Ltd. [1969] RPC 41, at p 47.

vi. Council of the Shire of Wyong v Shirt (1980) 146 CLR 40, at p 48.

vii. X v Y [1988] 2 All ER 648.

viii. See Tarasoff v Regents of the University of California 17 Cal 3d 425, 551 P 2d 334 (1976).

ix. Freedom of Information Act 1982 (Cth); Freedom of Information Act 1992 (Qld); Freedom of Information Act 1989 (NSW); Freedom of Information Act 1982 (Vic); Freedom of Information Act 1991 (SA); Freedom of Information Act 1989 (ACT); Freedom of Information Act 1991 (Tas) Freedom of Information Act 1992 (WA).