Protecting patient confidentiality in hospitals

Ea Mulligan

Ea Mulligan is Director of Medical Services, Repatriation General Hospital, Adelaide.

Abstract

As new methods of electronic data storage and distribution appear in hospitals, new challenges in protecting confidentiality have emerged. At the same time, demands for 'seamless' care and the desire to share information between clinicians are motivating hospitals to relax barriers to the transfer of patient information.

Increasing numbers of users at multiple sites compound the difficulty of ensuring information systems security. Hospital policy may demand that requests by patients to restrict the distribution of personal information be respected, while existing electronic systems are not able to deliver on this promise.

Compliance with the Information Privacy Principles of the Commonwealth Privacy Act 1988 *and the Australian Standard 4400–1995 'Personal privacy protection in health care information systems' will provide a useful framework for managing these challenges. However, their implementation will require some forethought.*

Introduction

Hospitals maintain a large volume and wide variety of patient records. As custodians of information, both on behalf of patients and of the staff who collect and record it, they have traditionally been very conservative in their policies concerning the release of patient information.

New methods of electronic data storage and distribution present new challenges in protecting the confidentiality of patient information. At the same time, demand for 'seamless' care which crosses organisational boundaries, and an awareness of the treatment errors which result from failure to transfer information effectively, have generated incentives to create new electronic linkages and reduce barriers to the transfer of patient data.

Current practice

Public hospital patients in all States and Territories except the Northern Territory may obtain copies of their own records through State or Territory freedom of information legislation. Hospitals routinely provide detailed information to a patient's general practitioner (discharge summaries and outpatient letters) and to other treating teams (other hospitals or community services) on request. Requests for information from other third parties are usually rejected, unless there is written consent from the patient or there is a legal compulsion to provide information. Unusual requests or those involving conflicting statutes are referred to an in-house expert or an external legal adviser.

Several paper-based medical records may be maintained. The most comprehensive of these are stored in the Medical Records Department when they are not required in a treatment area. There are many other locations at which paper copies of parts of the record may be held, and many departments maintain special registers or sets of notes. Each location is reasonably secure against casual access, despite the fact that some records must be retrieved by many different staff members (occasionally late at night).

Many members of the treating team contribute to the medical record. They create the record without seeking consent from the patient for subsequent release of information to third parties. In some areas where highly sensitive information is collected (for example, social work departments, sexually transmitted diseases clinics and abortion services), it may be part of routine clinical practice to discuss confidentiality and access to records explicitly with patients. This would only occur for a minority of hospital patients overall.

Current challenges

Extensive and evolving electronic information systems have produced multiple co-existing paper-based and electronic data collections in hospitals. It has become difficult to locate all of the records held by a hospital concerning a particular patient.

The electronic information systems have multiple access points and the capacity to allow one user to browse many records. An effect of this network of access points is that responsibility for protecting information has become widely distributed within hospitals. Preservation of confidentiality in the whole system requires that the large numbers of individuals who have become data users must also be reliable data custodians.

The combination of electronic records into central databases improves efficiency but simultaneously presents new risks to confidentiality. Methods for safeguarding electronic information are relatively new. Consequently, they are either unfamiliar or untested in the hospital environment.

The working assumption is that a combination of professional ethics, orientation of new staff to the local information systems, and ongoing training in the maintenance of confidentiality and data protection will ensure system security overall.

Hospital policies may optimistically require staff to act upon patient requests that information not be disclosed. Such special requests can be respected and acted upon by members of the treating team and any other staff members who become aware of it through the paper record or verbal instructions. In contrast, the technical features of electronic information systems may not be capable of attaching such a request to the data. Furthermore, many systems cannot selectively bar access to the data concerning one patient or one type of event in a patient's history. In practical terms, it is not possible to comply with a patient's request to restrict distribution of information about them.

The desire to improve care by ensuring that significant information is not withheld from service providers has stimulated initiatives in easier data transfer. The routine facsimile notification to a general practitioner on the admission of their patient is only one example.

The creation of large electronic 'data warehouses' within hospitals has been mirrored by the creation of multi-hospital repositories which hold information concerning patients from many hospitals. In these settings, numerous local systems are contributing to the creation of new combinations of patient information.

Future challenges

Large data repositories with many linked electronic sources will continue to be created. These may eventually form the nucleus of an entirely electronic medical record. Hospitals will wish to provide access to patient information to all of the clinicians treating each patient. Electronic transfer of this information will be the most efficient option, irrespective of whether all of the treating clinicians are at the same site or have the same employer.

Growing cooperation between institutions will provide opportunities for increased sharing of patient information. The systems which contribute to electronic information transfers will continue to have limited capacity to protect

confidentiality. They may be unable to selectively bar distribution of more sensitive information. They may be incapable of attaching to the data any indicator of the existence of consent to release the information – or lack of it.

Some of the risks which will appear are predictable. A complaint of a breach of confidentiality may lead to a requirement to change, upgrade or decommission existing electronic systems.

Hospitals will regularly have to consider the implications of proposals to link patient data in new ways and give access to new people. The results of these decisions will be the subject of scrutiny and debate. Patients (and their legal advisers) will expect to be able to discover all of the information about them that a health service holds.

Increasing numbers of users across multiple sites will increase the risk that information will be disclosed to the detriment of a patient. At the same time, the logistics of issuing selective systems access, providing training and auditing computer use will become more demanding and expensive as systems expand.

Consumer concerns

Some patients have a low level of trust in organisations. Among our potential or actual patients are members of the 'stolen generation' and survivors of the Holocaust. Others have experienced what would now be considered breaches of privacy in an era when more paternalistic values guided information release by government agencies.

There are patients with particular concerns based on a realistic appreciation that they could suffer discrimination or other adverse consequences flowing from a breach of confidentiality.

The only way to address these concerns is to be, and to be seen to be, irreproachable in our conduct.

In contrast, other consumers expect that all relevant information will be shared. They may become irritated when different providers repeat the same question. (Do you have any drug allergies? It is the left leg we will be operating on, isn't it?) Such individuals may complain when the information which they provide is not taken into account in subsequent treatment decisions.

We are aware that many patients will generously allow access to their personal information for research and other purposes not directly relating to their own health care (Dwyer 1997; Women's Health Australia 1997).

Legal environment

The Commonwealth *Privacy Act 1988* was framed to incorporate the obligations accepted by Australia under Article 17 of the International Covenant on Civil and Political Rights. The Information Privacy Principles (IPPs) contained in the Act also demonstrate Australia's commitment as a member of the Organization for Economic Co-operation and Development to take into account, in domestic legislation, principles concerning the protection of privacy and individual liberties set forth in the organization's 1981 guidelines (Attorney-General 1988).

The Privacy Act establishes rules of conduct in Commonwealth agencies for the collection, retention, access to, correction, use and disclosure of personal information. State/Territory legislation and departmental codes of conduct have generally been framed to maintain consistency with the Privacy Act. It is only one of a number of statutes which govern hospital practice in regards to release of information. There are numerous State and Territory laws which either require or prohibit release of particular types of information by hospitals or by medical practitioners working within them.

Professional ethics and personal duty of care

Individual service providers identify an ethical obligation to protect information disclosed to them in confidence. This personal responsibility is often expressed as being part of the duty of care to the patient.

Most service providers accept that the established practice of releasing information to a patient's other service providers (or transmitting it between members of the same team) is ethical because it is in the best interests of the patient. Patient care is optimised when all of the treating clinicians are fully informed about the patient. Disclosure for other purposes could result in a loss of trust in hospital treating clinicians as custodians of information.

Some medical colleges have sought to address the ethical problem confronted by medical specialists who must rely on the security of hospital information systems to protect the confidences of their patients. In a joint policy statement issued in 1995, the National Venereology Council of Australia, the Australian College of Venereologists and the New Zealand Venereological Society instructed that 'STD/sexual health service medical records should be kept separate from general hospital medical records'.

Hospitals can separate the information collected in certain services from an integrated hospital information system. The consequence will be that the segregated information will be excluded from ordinary hospital activities such

as statistical collections and coding, or a requirement for double entry will be created.

Undermining public confidence in the provider of health services

It is in the best interests of patients to provide full and accurate information to their treating practitioners. The ability to provide emergency care to recreational drug users, pre-anaesthetic screening which includes questions about alcohol and drug use, contact tracing for sexually transmitted diseases and needle exchange programs are all examples of services which rely upon the willingness of patients to divulge potentially incriminating information.

Threats to the public interest

There are potential threats to the public interest generated by either restricting or facilitating transfers of personal information. These pressures are being felt by the custodians of health information worldwide. In the United States, the chairman of the Congressional Technology Assessment Board warned that appropriate data security safeguards are essential (United States Congress 1995, p iii):

> *Otherwise concerns for the security and privacy of networked information may limit the usefulness and acceptance of the global information infrastructure.*

In Australia, the Privacy Act recognises that several public interests may be in competition when considering breaches of the Information Privacy Principles. Section 29(a) of the Privacy Act directs the Privacy Commissioner to:

> *have due regard for the protection of important human rights and social interests that compete with privacy, including the general desirability of a free flow of information and the recognition of the right of government and business to achieve their objectives in an efficient way.*

Creating new combinations of data

An area of particular concern is the linking of different kinds of information to create new combinations of data about individuals. In relation to this issue, section 17 of the Privacy Act restricts the use of tax file numbers to certain purposes, and prohibits their use for identifying individuals for other purposes. section 135A of the Commonwealth *National Health Act 1993* places restrictions against linking Medicare and Pharmaceutical Benefits Scheme claims and requires the functional separation of the two types of information (Human

Rights Commission 1992; Privacy Commissioner 1995, p 5) except in strictly controlled circumstances.

Information Privacy Principle 10 indicates that data collected for one purpose (for example, patient care) may not be used for another purpose (for example, costing studies) without seeking specific consent from the patients. In addressing this principle, the Australian Standard 4400 would require an independent review of ethical and privacy considerations before proceeding to link electronically stored information and generate new combinations of data.

Hospital responses

Compliance with the requirements of the Commonwealth *Privacy Act 1988* and the Information Privacy Principles contained within it, combined with those of the current Australian Standard 4400–1995 'Personal privacy protection in health care information systems' presents a significant challenge for hospitals.

Hospitals will need to consider the content of appropriate patient and staff education, construct a process for independent review of proposals to use data in new ways, commit to planning for the introduction of 'privacy capable' software, and maintain database registers. The standard will also encourage hospitals to adopt policies which harmonise with those of other agencies and to obtain explicit consent from patients for the transfer of health information between providers.

Patient education

A hospital employee collecting personal information from a patient should take reasonable steps to make them aware of the purpose for which the information will be used, anyone to whom the hospital would usually disclose this kind of information, and any third parties to whom they usually hand on information (IPP 2). Patients are entitled to have access to records about them (IPP 6) and may demand corrections or additions to inaccurate or misleading information (IPP 7). Information should not be passed on by a hospital except under force of law, where the patient has consented, or where they were reasonably likely to have been aware that information of that kind is usually passed on (IPP 11).

Careful consideration will need to be given to the methods by which these complex concepts should be explained to patients. We need to understand what the 'reasonable steps' are which a hospital should take to make patients aware of information disclosure policies. If done well, such educational measures will establish implied consent by patients for our current practices.

Staff education

New and existing staff members will require education concerning their responsibilities as information collectors and custodians. Collectors of personal information are responsible for ensuring that information is relevant, up to date and complete (IPP 3) and that the record is protected securely (IPP 4). They must also ensure that a register is kept of records held and that the patient can find out what records are kept, who the custodians of the records are, and who may have access to them (IPP 5).

Independent review

Information collected for one purpose may not be used for a different purpose without the express consent of the subject (IPP 10). Clauses 3.1 and 5.1.4 of the Australian Standard 4400 require a mechanism for the independent review of the information policies of hospitals and of individual proposals to use information for new purposes.

Institutional ethics committees represent a local source of expertise in teaching hospitals and are structured to provide independent determinations. Considering hospital policies and adjudicating on proposals which seek to use patient data in new ways or which breach one of the Information Privacy Principles are tasks which will be new to many institutional ethics committees. In a teaching hospital, this responsibility has the potential to add considerably to the program of work undertaken by ethics committees.

Clinicians have been hesitant to expose ordinary clinical practice to their review. This may be because the rigorous standards of data protection and consent required for research could be paralysing if they were applied to ordinary clinical settings.

Information systems planning

The need to mark, remove identifiers from or restrict access to some electronically stored patient information may require alteration of existing software. Such processes will consume resources and must be balanced against other demands. Seeking to introduce new software which has these capabilities will require both participation in the political process and a willingness to spend more on more technically complex capabilities.

Centralised purchasing gives individual health units an advisory role in establishing the need for particular functions. Purchasers should be advised that new information systems need the ability to identify information which patients have indicated requires special privacy measures. They also need to be able to

identify information which a patient has consented to release. This is the infrastructure required to act upon consent by patients to the electronic transfer of their information to clinicians outside the hospital.

Policy consistency with partners

There are clear advantages in adopting uniform policies on the release of information, especially when hospitals seek to share data with each other and with general practitioners. One of the requirements of the Australian Standard 4400 is that data should not be transferred to a 'trusted third party' unless they, in turn, adhere to the standard. The development of recognised standards by private sector partners has the potential to provide mechanisms for establishing 'trusted third party' status within regions. If it is adopted, the 1997 draft *Code of Practice for Medical Records in General Practice* under discussion within the Royal Australian College of General Practitioners may become such a tool.

Written consent from patients for the transfer of information

The risk in requesting consent from patients to transfer information is that it may imply a service which cannot be delivered. The request for consent suggests that the patient may not consent. Other than placing an alert in the paper-based medical record, it is not clear what additional steps a hospital is able to take to restrict the transfer of patient information on behalf of a patient who does not give consent. There is some information which must be collected in order to undertake administrative tasks such as generating a patient record. There are some electronic information transfers which cannot be blocked selectively. In this circumstance, rejection by one patient might precipitate the suspension of a whole class of information transfer, such as recording pathology results in a multi-hospital data repository.

Conclusion

Hospitals are confronting new challenges in protecting the confidentiality of patient information. There are new risks generated by expanding electronic information systems, the proliferation of multiple paper and electronic records, and the continuing pressure to improve patient care through increased information-sharing.

The Information Privacy Principles and the Australian Standard 4400 can provide health administrators with a useful framework for managing current risks as well as those which can be foreseen as information systems expand. Application of the principles and standard in hospital settings will require careful

thought. All new initiatives need to be considered in the context of the legislative and policy environment and with consideration of consumer, provider and broader public interests.

A number of steps which hospitals can take to meet these challenges have been proposed. Patient education concerning the intended uses to which information will be put can improve the quality of the implied consent upon which hospitals ordinarily rely. Improved staff education will be required as responsibility for data security spreads to a greater number of employees. Establishing a mechanism for independent review of hospital information policies and keeping a database register will be new tasks in many hospitals. The process of procuring privacy capable software will require some time to bear fruit, but will provide the infrastructure required to allow patients to give explicit consent to the electronic transfer of their own information to third parties.

All of these tasks will be addressed most effectively if health services seek to harmonise their information release policies. By adopting consistent standards, hospitals can facilitate rather than hinder the establishment of 'trusted third party' relationships between information-sharing partners.

References

Attorney-General 1988, *Explanatory Memorandum to the* Privacy Bill 1988, Australian Government Publishing Service 15389/88, Cat No 88 51796.

Dwyer J 1997, 'Privacy versus the collective good', *Australian Health Review*, vol 20, no 1, pp 21–3.

Human Rights Commission 1992, *Medicare and Pharmaceutical Benefits Programs Privacy Guidelines,* Report by the Privacy Commissioner to Parliament under Section 135AA, National Health Act, Canberra.

National Health Act 1993, Commonwealth of Australia, Canberra.

Organization for Economic Co-operation and Development 1981, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,* Paris.

Privacy Act 1988, Commonwealth of Australia, Canberra.

Privacy Commissioner 1995, *Medicare and Pharmaceutical Benefits Programs; Privacy Guidelines 1994,* Human Rights Australia, Sydney, New South Wales.

Standards Australia 1995, *Australian Standard; 'Personal privacy protection in health care information systems',* AS 4400–1995, Homebush, New South Wales.

United States Congress 1995, *Information Security and Privacy in Network Environments,* Office of Technology Assessment, OTA-TCT-606, Washington DC, September 1994.

Women's Health Australia 1997, *Women's Health Australia Newsletter,* University of Newcastle, Callaghan, New South Wales, March.