Asia Pacific Family Medicine 2002; **1**: 37–40

DISCUSSION PAPER

Global access to patient information

Richard WHIDDETT,[1] Jocelyn HANDY[2] and Inga HUNTER[3]

[1]*Department of Information Systems and* [2]*School of Psychology, Massey University, and* [3]*Independent Family Practitioner, Palmerston North, New Zealand*

Abstract: Electronic information storage and communication systems facilitate the transfer of information between different people and locations. Effective communication between systems is dependent on all the components adhering to common technical standards, such as the Internet standards. Recently there has been a lot of work on the development of standards for information and communications systems that are suited to the health sector. As these developments mature, it may be possible for healthcare professionals to have instant access to information about their patients from systems throughout the country, or even around the world without leaving their consulting rooms. Similarly, in their absence, someone else may be able to seek information from their systems. This paper explores some of the social and cultural implications that arise from the increased dissemination of personal information via these systems. The discussion highlights the need for flexible and adaptable standards and mechanisms to control the access to patients' information.

Key words: communication systems, confidentiality, electronic medical records, patient information.

Introduction

For many years, healthcare professionals have been using information systems to improve the efficiency and effectiveness of their delivery of patient care via electronic administration systems and electronic medical records (EMR).[1] These systems were initially used in secondary care, where the high costs involved in setting up and maintaining them could be more easily absorbed. However, with the fall in technology costs and the trend for healthcare practitioners to work within groups, their use has increased in primary care. Initially systems focused on improving practice administration, but now primary care practitioners are expanding these systems to include EMR.

Electronic communications systems and computer networks are also being used to link these information systems with other parts of the health sector. Increasingly, the primary care sector is using electronic systems to:

- order diagnostic tests and receive the results
- deliver prescriptions
- exchange admission and discharge letters with secondary care institutions
- lodge claims for payment.

These linkages have the dual benefits of improving patient care by increasing the speed and reliability of information exchange and reducing administration costs.

It is becoming feasible to develop a 'virtual' lifelong electronic medical record of a patient.[2] With this technology a complete medical record no longer needs to be stored in one location; instead, a virtual record could be constructed by piecing together the jigsaw of a patient's history scattered throughout various information systems. With such a system, a healthcare professional anywhere in the world could access all the information about a patient by simply entering a patient's identification.

Although such a system may sound futuristic, much of the required technological infrastructure is either in place or being developed. In order to exchange information, information systems need to share common formats for encoding and storing information within the medical record. Technical standards for communication systems also need to ensure the security of the systems during message exchange. The European

Correspondence: Dr RJ Whidett, Department of Information Systems, Massey University, Private Bag 11 222, Palmerston North, New Zealand.
Email: r.j.whiddett@massey.ac.nz

Accepted for publication 14 October 2001.

Standards Committee (CEN) and the Health Level Seven, Inc. (HL7) have undertaken much of the work to develop the technical standards.[3,4] The work is now being consolidated by the International Organization for Standardization (ISO) Technical Committee on Health Informatics and a series of technical international standards relating to the storage and communication of patients' information are expected to emerge over the next few years.[5,6]

In general, these committees have tended to focus on the technical aspects of systems rather than examining the ethical and social issues that are associated with the distribution of patients' information. An important issue for practitioners is that the emerging standards are flexible enough to facilitate the use of technology in a way that meets their needs without dictating or constraining the way they practice medicine.

Importance of privacy

Although the potential benefits of health information systems are widely accepted, the potential threats to confidentiality with its implications for patient privacy, are more controversial.[7]

Confidentiality

This is essential to the patient–physician relationship. Unless a patient can be sure that personal information will not be distributed against their wishes, they may be reluctant to disclose sensitive information which may be crucial for correct treatment. Proponents of EMR systems argue that paper records are inherently insecure anyway as they can be browsed or copied by anyone who handles them without leaving any trace of their actions. In contrast, EMR systems can have security mechanisms, access controls and audit logs built into them which restrict and report on such breaches of confidentiality.

Unfortunately, there are two major problems with computer based records:

- First, individual records can be accessed from a remote location making them potentially more vulnerable to breaches of privacy;
- Second, computer-based systems facilitate sophisticated searching and record matching operations which can breach privacy in ways not possible with paper-based systems.

Threats to privacy

These kinds of threats to personal privacy are neither new or unique to healthcare. As long ago as 1980, the Organisation for Economic Co-Operation and Development (OECD) published a series of guidelines to control the flow of personal information of any kind across international borders.[8] These basic principles have been adopted into the legislation of many western nations (e.g. Australia, Canada, New Zealand and the United Kingdom), although the details of the implementation vary. However, some countries still do not have sound laws to protect people's privacy. Even with legal protection, however, concerns over patient privacy remain. In 1997 the British government commissioned the Caldicott Enquiry to examine the privacy issues related to the exchange of patient information, producing a number of recommendations to improve patient privacy.[9]

Several writers have argued that the ideal situation would be for the patient to have complete control over who accesses each part of their health information.[10,11] A number of proposals have suggested mechanisms for implementing these access controls, for example, the CEN standard proposes that each unit of a patient's record should have a 'distribution list' associated with it, defining who may see the information. However, such a system may be rather cumbersome and impractical to implement due to the enormous amount of administration and maintenance required. Most of the currently available systems tend to work on an access control matrix, shown in Table 1. One dimension of the matrix identifies the various categories of information, or sections of a patient's record which are to be

Table 1 An access control matrix

	Categories of information				
	Demographic	**General history**	**Prescriptions**	**Sexual health**	**Etc.**
Roles					
Family practitioner	✔	✔	✔	✔	. . .
Consultant	✔	✔	✔	✘	. . .
Pharmacist	✔	✘	✔	✘	. . .
Administrator	✔	✘	✘	✘	. . .
Etc.	. . .	. . .	. . .	. . .	. . .

controlled. The other dimension defines the various roles which a person may be fulfilling when they are accessing the information, for example, family practitioner, consultant, administrator, etc. The access rights for each role can then be defined. In the example in Table 1, an administrator would only have access to demographic information about patients, while a pharmacist would also have access to information about their prescriptions.

Clash of cultures

Unfortunately, several problems prevent the development of a universally acceptable access control policy based on the standard access control matrix.

Who has access?

Many areas of sensitivity are defined by the surrounding culture. The contentious issues relating to information access often arise when a conflict of interest exists between the individual patient and other individuals, a group of people or society as a whole. Examples include the rights of adopted children and their parents, immunization records, HIV status and DNA fingerprinting. In each of these areas, a different policy might be adopted depending on the weighting that society places on individual privacy verses the interests of others. For example, traditional New Zealand Maori regard the obligations and responsibilities of the extended family relationships, or whanau, as much greater than is usual in a conventional western society. Consequently, members of the whanau sometimes expect greater access to the health information of other family members than is permitted under New Zealand's western-based privacy laws.

The need for discretion in different cultures

Certain issues, for example sexual or social history, may be extremely contentious in one culture, but not so much in another. This means that selective control (i.e. the columns in Table 1) of certain categories of information within a patient's record and the access profile for a particular role, may be different for different cultures. The New Zealand Privacy Commissioner recently reported an example of this.[12] A Fijian student studying in New Zealand was cut off by her family when aspects of her health information were leaked to her family by a distant relative who worked in the hospital. This situation arose partly because the hospital did not fully appreciate the degree of privacy required in a Fijian culture.

The role of healthcare delivery

The roles that exist (i.e. the rows in Table 1) or the access requirements for a particular role may differ between institutions or countries because of the way that healthcare is delivered. For example, in different countries the role of nurses or midwives may vary and thus their profile of access rights would also vary depending on the level of responsibility they are expected to assume.

Any access control mechanism based on a matrix approach will therefore need to be customized to define the categories of information, the access roles and the access profiles that are appropriate to the local culture and customs.

Difficulties may also arise when records are transported across cultural boundaries, with appropriate adjustments needed for the new context. An added problem may be that a different judicial context may not offer the same protection for the privacy of the individual patient. Although the above case of the Fijian student did not arise because of these new technologies, similar cases are much more likely to occur as personal information becomes more readily accessible from remote locations.

Conclusions

While the development of new information and communications technologies are bringing many benefits for both patients and organizations, they raise a number of unresolved issues relating to patient privacy and access to patient information. When paper-based records or isolated computer systems are used, the practitioner has some discretionary control over what information to reveal to other parties. However, the automation of the process of accessing patient records will remove this opportunity to exercise discretion on an ad hoc basis and a more formal approach will be needed.

This issue has implications for designers of information systems, for healthcare professionals and for individual patients.

Designers of information systems should not build in a specific access control policy as it may render the system unusable in another context. Systems will need to be flexible in order to accommodate the differing categories of information, differing roles and differing access control profiles that are required to meet the varying organizational and cultural needs of different societies.

More debate and clarification is needed about the policies and rules that apply to the release of personal health information so that systems are designed to meet the needs of both practitioners and patients.

References

1 Hovenga E, Kidd M, Branko C (eds). *Health Informatics: An Overview*. Churchill Livingstone, Melbourne, 1996.
2 Mount CD, Kelman CW, Smith LR, Douglas RM. An integrated electronic health record and information system for Australia? *Med. J. Aust.* 2000; **172**: 25–7.
3 European Standards Committee (CEN). European Standardization of Health Informatics. http://www.centc251.org.
4 HL7 Consortium. Health Level Seven. http://www.HL7.org.
5 International Organization for Standardization (ISO). International Organization for Standardization. http://www.iso.ch/iso/en/ISOOnline.frontpage.
6 ISO Technical Committee on Health Informatics. ISO/TC 15 on Health Informatics. http://www.astm.org/COMMIT/ISO/tc215.html.
7 Carter M. Integrated electronic health records and patient privacy: possible benefits but real dangers. *Med. J. Aust.* 2000; **172**: 28–30.
8 OECD. Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. http://www.oecd.org/dsti/sti/it/secur/prod/.
9 The Caldicott Committee. Report on the review of patient-identifiable information 1997. http://www.doh.gov.uk/confiden/crep.html.
10 Anderson RJ. *Security in Clinical Information Systems*. BMA, London, 1996.
11 Mandl KD, Szolovits P, Kohane IS, Markwell D, MacDonald R. Public standards and patient control: how to keep medical records accessible but private. *BMJ* 2001; **322**: 283–7.
12 Privacy Commissioner. New Zealand Health Waikato Investigation. http://www.privacy.org.nz/shealthf.html.