Information in practice

Privacy in clinical information systems in secondary care

Ian Denley, Simon Weston Smith

System C,
Maidstone
ME14 1SR
Ian Denley,
senior analyst

Conquest Hospital,
St Leonard's on Sea
TN37 7RD
Simon Weston
Smith,
*consultant
haematologist*

Correspondence to:
Dr Weston Smith
simon_weston_
smith@
compuserve.com

BMJ 1999;318:1328–31

Summary points

The electronic patient record threatens to make private health information readily available for misuse

Principles can be applied to the electronic patient record to maximise privacy, but professionals in healthcare information technology have been reluctant to adopt these principles on the basis that they would be expensive to implement and unwieldy to maintain

Failure to adopt adequate security may prove to be even more expensive, however

Fundamental to patient privacy is the need to control access to each patient's electronic record

This can be achieved by matching a patient's current clinical contacts with a user's rights; this has been shown to be workable in a hospital-wide clinical information system

Two years ago *Sunday Times* reporters were able to gain access to the private medical records of Dr Sandy Macara by paying a small fee to a commercial agency. As computerised clinical information systems that are capable of holding large amounts of high quality information become more widespread in NHS trusts, the privacy of patient information is becoming an increasingly important issue. Lack of privacy can be damaging to both the patient and the organisation concerned. For example, Barber cites the following problems[1]:

- Personal safety
- Infringement of personal privacy
- Loss of public confidence in the organisation (such as an NHS trust)
- Failure to meet legal obligations
- Financial loss and disruption of activities.

In the BMA consultation document *Security in Clinical Information Systems* Anderson identifies nine principles governing the design of a clinical information system meeting the requirements for patient privacy.[2] Doubts have been raised about the feasibility of adopting the code for governing access to patients' electronic records in secondary care. Our experience is that the principles are achievable.

This article is based on our experience of a large scale clinical information system in use in three British hospitals—Conquest Hospital, Hastings; Aintree Hospital, Liverpool; and Royal Devon and Exeter Hospital, Exeter. We describe the approach taken to ensuring control over access to confidential patient information on the basis of expected relationships between staff and patients.

Overview of clinical information system

The clinical information system under discussion goes a long way to providing a fully integrated electronic patient record. Briefly, it includes traditional clerical information about appointments and admissions; results from specialties such as pathology, radiology, and endoscopy; drug treatments; procedures; and problem lists. In addition, it generates and stores plans for nursing care, clinical correspondence, and dictated notes from ward rounds. Paper notes are no longer required in some clinical areas.

Access control

The first three principles listed by Anderson identify the need for a clinical information system to limit a user's access to the records of his or her own patients and no others. Anderson proposes that this is done through access control lists that identify which individual users are responsible for a patient. He further proposes that a single user will have responsibility for a particular patient's access control list. In the secondary care setting, where a patient benefits from input from several professionals from different specialties and disciplines, often in an emergency, a manual implementation of these access controls is not tenable. We have taken an approach that recognises the team based way in which care is delivered in secondary care. The system makes use of the clinical information system's knowledge of a patient's hospital contacts to decide whether an individual user, working as part of one or more teams, in one or more places, should be allowed access to an individual patient's record.

In order to achieve this, users are identified to the clinical information system as having one of a number of roles such as ward based nurse, specialist nurse, junior doctor, ward clerk, medical secretary, clinical consultant, physiotherapist, pathologist, radiologist, etc. Users are granted rights to particular wards, consultants, or specialties. Users are also optionally granted rights to subsets of data within an individual patient's record or any of a number of task based rights.

For the patient, all past, current, and future clinic appointments, admissions, referrals, and other contacts are known to the system.

Examples of how this information is applied:

- A ward based nurse is able to access information only on patients currently on any of his or her allocated wards or on any of these wards in the past 30 days. This has the disadvantage that when a patient or general practice telephones a ward with a legitimate request for information about a patient discharged over a month ago a ward nurse is not able to provide it from the clinical information system.
- A doctor or specialist nurse is able to access the notes only of patients currently under the care of any of the consultants with whom he or she is working. The number of teams to which a doctor may be allocated can be as few as one or as many as all the teams in the hospital trust. In practice, junior doctors are provided with access to all the consultant teams in their directorate to ensure that they are able to access information for the patients they will cover on call. In consequence, opinions required on call from members of other directorates—such as a medical opinion requested on a surgical patient—may require the medical registrar to exercise override access to that patient's notes.
- A ward clerk is able to access the clerical information on patients on his or her ward but may not be allowed access to previous clinical correspondence. Sensitive subjective opinions as expressed in correspondence may not be thought to be the domain of the ward clerk.
- We have described the technical details of the system of access control elsewhere.[3]

Nine principles of data security (from Anderson[2])

(1) *Access control*—Each identifiable clinical record shall be marked with an access control list naming the people or groups of people who may read it and append data to it. The system shall prevent anyone not on the list from accessing the record in any way.

(2) *Record opening*—A clinician may open a record with himself or herself and the patient on the access control list. When a patient has been referred the clinician may open a record with himself or herself, the patient, and the referring clinician(s) on the access control list.

(3) *Control*—One of the clinicians on the access control list must be marked as being responsible. Only this clinician may change the access control list, and he or she may add only other healthcare professionals to it.

(4) *Consent and notification*—The responsible clinician must notify the patient of the names on his or her record's access control list when it is opened, of all subsequent additions, and whenever responsibility is transferred. The patient's consent must also be obtained, except in emergency or in the case of statutory exemptions.

(5) *Persistence*—No one shall have the ability to delete clinical information until the appropriate time has expired.

(6) *Attribution*—All accesses to clinical records shall be marked on the record with the name of the person accessing the record as well as the date and time. An audit trail must be kept of all deletions.

(7) *Information flow*—Information derived from record A may be appended to record B only if B's access control list is contained in A's.

(8) *Aggregation control*—Effective measures should exist to prevent the aggregation of personal health information. In particular, patients must receive special notification if it is proposed to add a person to their access control list who already has access to personal health information on a large number of people.

(9) *Trusted computing base*—Computer systems that handle personal health information shall have a subsystem that enforces the above principles in an effective way. Its effectiveness shall be evaluated by independent experts.

Attribution

In line with the sixth principle listed by Anderson, the system also keeps an audit trail of all occasions when a patient's record is accessed regardless of whether any information is altered. A separate and full trail of all changes is also maintained, making it possible to recreate the sequence of actions undertaken by a user. Users' knowledge of the existence of these audit trails, together with the fact that inappropriate access to private information is a dismissable offence, goes a considerable way to discouraging misuse of the system.

Need for security override

This approach effectively controls access in line with working practices, but it does require the system to know about the teams responsible for a patient in order to assign access rights. Occasionally, the system will not be aware that a team is responsible for a particular patient's care, and members of that team may be denied access to the patient's record. In order to handle this eventuality, certain users may be granted "override" privileges, which allow them to gain access to a set of notes.

As currently implemented in Hastings, this facility is available to all medical users and clinical secretaries but not to ward based staff. When a user with override privileges asks for the electronic record on a patient for whom the system can find no user-patient association, the following text appears: "You do not work with any of the people known to be responsible for this patient and should not therefore open their notes. You may override this security measure if you are genuinely involved in this patient's care. Please be aware that a record of who, where, and when is taken every time a patient's electronic notes are opened."

The user is then asked to leave this patient's notes unopened but is also presented with the options to formally establish a new carer for the patient or to open that patient's notes regardless. The exercise of this override facility generates an entry in a separate audit trail, which can be closely monitored to detect misuse. Currently, roughly 50 overrides are requested each day from diverse areas such as microbiology, where the lack of computerisation means that the clinical information system has no data on which to base decisions about user-patient relationships, and from endoscopy, where referrals are received before any administrative user-patient relationships are identified.

Subsets of patient information

In addition to the nine principles of data security, we have taken a formal approach to problems that arise when certain elements of a patient's clinical record may be deemed to be sensitive. For example, psychiatric correspondence may be marked as confidential or highly confidential. In the latter case only the author, recipient, and typist are aware of the letter and its contents. In the former case, only members of the author's and recipient's teams may see the letter. A further example is provided by the child protection register. In this case the user is alerted to the possibility that a child may be on the register when the patient's notes are opened, but further details about the child's protection status are withheld unless the user is one of the few who have rights to the register. The normal user is advised to seek further information from the child protection office as necessary to clarify the nature of the entry.

This approach can also be extended to areas such as appointments at sensitive clinics or drug prescriptions that clearly indicate a particular diagnosis. The problem with limiting access to the latter sort of information is the obvious one of hiding a dangerous drug interaction. We have not resolved this, but one solution is for the system to advise of a drug interaction without identifying the relevant drug, leaving it to the clinician to discuss this directly with the patient.

Clinical audit

The need for patient privacy at some point comes into conflict with the benefits to be gained from sharing clinical information for educational purposes or for planning and delivering clinical services for a community. This is well understood by clinicians in the subject of clinical audit. This requires the aggregation of personal health information, and indeed the aggregation of clinician based information.

The principles listed by Anderson limit this sort of aggregation, certainly with regard to personally identifiable clinical information, and we currently still adopt this approach. Thus, a user asking audit questions of the system will be supplied with information only on patients to whom he has access. Patients who would otherwise match his audit inquiry are not listed. This has the advantage of ensuring patient privacy while still providing an efficient means of allowing the rapid review of notes, but it causes problems if you are trying to plan care for a group of patients with a particular problem, some of whom have not been under your care. For example, a diabetologist wishing to argue a case for improving the care for diabetic patients will be provided only with information on patients already known to him or her. Patients with a diagnosis of diabetes not formally referred for his or her opinion will remain hidden.

An alternative approach to this is for the system to extract statistical data without patient identifiers, but you then lose the ability to investigate individual cases in greater depth. This facility for anonymising data is only now being introduced to the system, and we cannot comment on its practical implementation.

Users' experience

Initial implementation of this system was met by comments from clinicians such as, "What's all this cloak and dagger stuff?" This scepticism about the importance of patient privacy has evaporated as users have become aware of the depth and breadth of information that is immediately available on their patients and the recognition that, without such measures, their own and their family's medical histories are all too readily available for casual browsers.

On the other hand, patients remain remarkably trusting of the uses to which their information may be put. While the system is able to produce a report of all accesses of an individual patient's notes, there has not yet, in five years, been a single request by a patient for such a report.

Conclusion

We have described an approach to managing patient privacy in a large scale clinical information system in the secondary care sector. The traditional approach of providing access to hospital staff to information on all patients has not been considered to be acceptable. Access to individual patient records has been made the key to the system with this access being granted only when the member of staff's rights match a patient's current clinical contacts. This approach has delivered a pragmatic and effective means of ensuring patient privacy.

We thank all the clinical, secretarial, and managerial staff in Hastings, Aintree, and Exeter who have contributed to discussions about the privacy of information in their hospital systems.

Contributors: SWS initiated the work on privacy reported in this article and put the building blocks in place at a practical level at the Conquest Hospital. ID coordinated the development and enhancement of the work across all three hospital sites and managed the development of the software. Both authors jointly formalised the ideas and contributed equally to the writing of the article. SWS is guarantor for the article.

Funding: None.

Competing interests: ID is an employee of System C, and SWS owns shares in System C. System C is a supplier of hospital information systems.

1 Barber B. Security and confidentiality issues from a national perspective. In: Barnett D, ed. *Patient privacy, confidentiality and data security. Papers from the British Computer Society Nursing Specialist Group Annual Conference, 1995.* London: British Computer Society, 1997.

2 Anderson RJ. *Security in clinical information systems.* London: BMA, 1996.

3 Denley I, Weston Smith S. Implementing access control to protect the confidentiality of patient information in clinical information systems in the acute hospital. *Health Informatics J* 1999;4:174-8.

(Accepted 23 October 1998)

Commentary: Let's discuss wider social and professional issues

Martin Gardner

Information Retrieval Research Group, Department of Computing Science, University of Glasgow, Glasgow G12 8QQ

Martin Gardner, *clinical research fellow*

martin@dcs.gla.ac.uk

The confidentiality of computerised clinical information systems can be violated either by illegitimate users ("hacking") or through inappropriate access by legitimate users. Currently, the typical approach to preventing the latter form of misuse relies on the principle of deterrence, which in turn depends on a combination of credibility of detection and fear of punishment. Each user of a hospital information system is provided with a login identity and a password. All have unlimited "Read" access to patient records, but "Write" access might be partially limited by task (for example, so that only doctors can prescribe drugs). Deterrence measures are relatively easy to implement and maintain. However, although audit trails permit easy confirmation of inappropriate access suspected on other grounds, in themselves they are not especially powerful as a means of detection.

A better approach is the principle of denial, such that inappropriate access is not merely detectable and punishable but is impossible. However, a workable policy of denial is much more difficult to implement and maintain, since in modern hospital practice the criteria for judging the legitimacy of information access are complex and highly dynamic and denial is potentially dangerous. (Who would be liable if an instance of information denial resulted in avoidable morbidity?). Denley and Weston Smith show that, in large scale hospital systems, it is feasible to implement a policy of denial for many clinical information users, together with enhanced deterrence for users who are allowed to override denial. This should be applauded.

However, as is so often the case in modern medicine, social and professional issues rise to the surface in the wake of technical advance; for example, with respect to policing responsibility, disciplinary procedures, and compensation. One of the most important social issues is that, while we are proposing that patients' taxes fund sophisticated computer systems to protect the privacy of patient data, it is evident that patients are largely unconcerned by the issue. Given a choice, most might prefer to fund services.

I suggest that the case for such systems is strong but that it is not best promoted by the dramatised anecdotes with which it is often illustrated, involving celebrity patients, embarrassing diseases, and exploitative strangers. Ordinary patients do not see themselves as being at risk in this way. A more subtle but far more compelling justification is that lack of privacy can cause insidious but widespread damage to relationships even when embarrassment or malice is entirely absent: for example, when colleagues know the result of your relative's breast lump biopsy before you or when a manager learns of an employee's pregnancy from someone other than the employee. A hospital is part of the community that it serves, and working relationships within hospitals are particularly vulnerable to such damage.

Perhaps the importance of the approach described is not that it is a final solution to the problems of confidentiality but rather that it represents a tool for building solutions. Given this capability, perhaps there is now a need for a wider debate on the social and professional issues raised.

Commentary: Organisational and cultural aspects are also important

Rory O'Conor

Clinical Audit Department, Pinderfields Hospital, Wakefield WF1 4DG

Rory O'Conor, *consultant clinical epidemiologist*

rory.oconor@panp-tr.northy.nhs.uk

Denley and Weston Smith describe a technical approach to controlling access to clinical information systems in secondary care. They recognise the team based method of clinical care in hospitals, and their approach enables access by individuals with legitimate team roles. This is not the same as limiting access to named individuals, but it may be closer to current practice in hospitals. The size of clinical teams, the stability of the team membership, and the urgency of access to information is different in primary care and secondary care. Solutions developed in one setting may not be appropriate or practical in another setting, even if the underlying principles are the same.

Their approach addresses some of the issues in an operational clinical setting but seems to be overly restrictive in secondary areas such as clinical audit, where it may be possible to share more clinical information by reducing the amount of private information included.

The Caldicott report clarifies some of the issues associated with privacy and clinical practice.[1] The new European Union directive on data protection (95/46/EC) provides a new legal framework, and *Health Service Circular 1998/153* states the current legal position in hospitals. These documents need to be read in association with reports from the BMA[2] and guidance from the General Medical Council.

The NHS Information Strategy *Information for Health* identifies some key elements of infrastructure where this debate needs to be developed, including the NHS network, the NHS number, telemedicine (such as NHS Direct), and interorganisational electronic health records as well as electronic patient records.[3] The document is high level and does not address privacy in any detail or issues such as encryption. There are additional issues in sharing healthcare information with other agencies such as social services or the police.

While access control is one approach to securing privacy, there are other options such as measures to reduce casual disclosure that does not contribute to care, the decoupling of private and clinical information in electronic records, and the use of various levels of anonymisation from name and address through identification by hospital number to full anonymity as part of an aggregate data set. As new technologies develop—such as digital images and web services—new issues will arise.

Privacy is often confused with confidentiality and secrecy. Some arguments about privacy may be more about openness and disclosure. Any healthcare encounter includes a compromise between maintaining privacy and enabling care. There are costs associated with different security solutions. We need to identify solutions that are socially acceptable, practical, and affordable.

Good security design of information systems will be part of the solution. Appropriate organisational procedures and the right cultural approach will be necessary for any technical solution to work. Denley and Weston Smith seem to have made good progress.

[1] Department of Health. *Report on the review of patient-identifiable information (Caldicott Committee).* London: DoH, 1997.
[2] Anderson RJ. *Security in clinical information systems.* London: BMA, 1996.
[3] Department of Health. *Information for health.* London: DoH, 1998.