Implementing access control to protect the confidentiality of patient information in clinical information systems in the acute hospital

I. Denley and S. Weston Smith

In this paper, a practical approach to managing the confidentiality of patient information in large-scale clinical information systems in the acute hospital is described. The traditional approach of limiting the functions that hospital staff can undertake is necessary but not sufficient. Control over access to the individual patient is required, with this access only being granted when the member of staff's rights match a patient's current clinical contacts. In our experience, the setting-up and maintenance of such rights is a non-trivial, but achievable, task.

Ian Denley
System C Healthcare Ltd
60–61 High Street
Maidstone
Kent
ME14 1SR
Tel: 01622 691616
Fax: 01622 691241
Email: ian@systemc.com

Simon Weston Smith
Consultant Haematologist
Conquest Hospital
The Ridge
St Leonard's on Sea
East Sussex
TN37 7RD

1NTRODUCTION

The National Health Service (NHS) information technology (IT) strategy 'Information for Health' [1] makes it clear that the UK government sees that 'the confidentiality of patient information is of paramount importance'. The means of ensuring this confidentiality are to be developed over the period of implementation of the strategy.

Within an acute hospital clinical information system (CIS), there are two major threats to this confidentiality.

1. The first is that posed by authorized users of the system who look at an individual patient's information for reasons other than the care of the patient. This may be driven by curiosity about the medical problems of an acquaintance.
2. The second arises where there may be a value to information, for example a list of names and addresses of patients with a hearing impediment to a hearing aid supplier, or a list of patients with malignant disease to a would-be employer.

A theoretical approach to countering these threats has been provided by the British Medical Association (BMA) consultation document 'Security in Clinical Information Systems' [2]. In this document, Anderson identifies nine principles governing the design of a CIS meeting the requirements for patient privacy. This paper describes a practical implementation of these principles based on the experience of a large-scale CIS in use in three hospitals in the UK (Conquest Hospital, Hastings; Aintree Hospital, Liverpool; Royal Devon and Exeter Hospital, Exeter).

OVERVIEW OF THE CLINICAL INFORMATION SYSTEM

The CIS under discussion goes a long way to providing a fully integrated electronic patient record. As a synopsis, it includes traditional clerical information about appointments and admissions, together with results from areas such as pathology, radiology and endoscopy. Drug treatments, procedures and problem lists are also maintained. In addition it generates and stores plans for nursing care, clinical correspondence and dictated ward round notes. Paper notes are no longer required in some clinical areas.

With regard to confidentiality, the operational CIS has three features of relevance:

- *Patient Master Index (PMI)* – a database of all patients who have ever attended the hospital.
- *Patient lists* – lists of patients on particular wards, attending particular clinics, etc.
- *Electronic casenote* – a flexible and configurable record of both clinical and clerical information associated with a particular patient (e.g. diagnoses, medications, demographic details).

Given these three features, so as to maintain the confidentiality of patient information, the CIS controls access to patient data in two ways:

- *By controlling access to patients* – a patient must be accessed before any information about them can be viewed; the CIS, therefore, controls which patients a user may see on their patient lists or may select from the PMI. These controls are based on rules about when it is legitimate to see a patient

and who should be able to see them (see the section 'Controlling access to patients').
- *By controlling access to discrete classes of information within a patient's electronic casenote* – different types of users have different information needs about a patient. The electronic casenote can, therefore, be tailored according to what a user needs to know about a patient. In practice, this means that users (or more often groups of users) are allocated rights to different parts of the electronic casenote on a 'section-by-section' basis (see the section 'Controlling Access to Components of a Patient's Electronic Casenote').

CONTROLLING ACCESS TO PATIENTS

The primary mechanism whereby the CIS determines whether a patient's information should be available to a member of staff, is by matching the member of staff's confidentiality profile with the patient's known contacts with the hospital. This technique is used to control which patients a user can see on a patient list (e.g. a ward list) and which patients a user can select from the PMI. Access control in both these situations is discussed below.

Controlling which patients are seen on patient lists

In many circumstances, hospital staff can access patients via patient lists. The CIS employs different types of patient lists, including: current in-patients; recent in-patients; current out-patients; recent out-patients; patients pending admission; and so on. Users can be granted access rights to one or more of these list types.

Importantly, however, which patients can be seen on these lists is controlled by a further layer of access rights, namely:

- *Ward/clinic rights* – limiting the ward/clinics to which the user has access.
- *Specialty rights* – limiting the specialty/specialties to which the user has access.
- *Consultant rights* – limiting the consultant(s) to which the user has access.
- *No restrictions* – allowing specific users to see all patients without restriction.
- *Temporal rights* – limiting access to patients with a current or recent episode.

Appropriate combinations of rights and patient lists will allow each user to access only those patients in whom they have a legitimate interest. The only exception is when the user has been granted a 'confidentiality override' facility (see the section 'The need for confidentiality override').

Controlling which patients can be selected from the PMI

In many instances (e.g. when admitting a patient, booking a new appointment, answering an enquiry about a recent patient), a user will want to be able to search for and select a patient from the PMI, which holds the details of all patients who have ever attended the hospital.

Because it allows the user to search accurately for an individual among hundreds of thousands of patients, the PMI is a powerful tool, the use of which must be strictly controlled and monitored to prevent abuses (such as searching for information about colleagues in the hospital).

The PMI displays only the minimum amount of information necessary to identify a patient unambiguously: that is, the patient's: name; sex; date of birth; unit number; and address. Access to other details, such as religion, ethnicity, telephone number, episode and event history, and clinical information itself is controlled. This is achieved by ensuring that users are only able to select a patient from the PMI search screen if:

- the patient has a current/recent episode; and
- the user's ward /specialty/consultant rights match the ward/specialty/consultant that the patient was under in any of their current/recent episodes.

If these two conditions are not met, the user is denied access to the patient's details. The only exception is when the user has been granted a 'confidentiality override' facility (see the section 'The need for confidentiality override').

ATTRIBUTION

In addition to the above measures, the system keeps a confidentiality audit log of all occasions on which a patient's record is accessed, regardless of whether any information is altered. This log allows those responsible for ensuring the confidentiality of patient information held on the computer system (e.g. Caldicott Guardians), to find out which users have accessed which patient's records and when, and whether this access involved the use of a confidentiality override. The confidentiality audit log can also be used to respond

to a patient's request for a list of all those people who have read their notes.

The interval between recording patient accesses (e.g. all accesses, daily, weekly, monthly) can be varied according to requirements, and accesses to a patient's record are recorded in the confidentiality audit log, which can be interrogated by:

- Patient – Allowing accesses to a particular patient's record to be examined. If no patient is specified, all patient records satisfying the remaining criteria will be included in the audit.
- User – Allowing audits to be conducted upon particular system users.
- Date – Allowing audits to be conducted for particular dates.
- Overrides only – Allowing audits to be conducted upon either overrides only or all accesses.

The audit log also displays the first and the last access to a particular patient by a particular user.

In addition, a separate and full trail of all changes is also maintained, making it possible to recreate the sequence of actions undertaken by the user.

The users' knowledge that these audit trails are in place, together with the knowledge that inappropriate access to private information is a dismissable offence, goes a considerable way to discouraging abuse of the system.

THE NEED FOR CONFIDENTIALITY OVERRIDE

The approach to protecting patient confidentiality described so far 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. On occasions, 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 that patient's record. In order to handle this eventuality, certain users may be granted 'override' privileges that allow them to gain access to a set of notes. As currently implemented in Hastings, this facility is available to all medical users and some 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 confidentiality 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 option to establish a new formal carer for the patient or to open that patient's notes regardless.

The exercise of this override facility generates an entry in the confidentiality audit log, which can be monitored to detect abuse.

CONTROLLING ACCESS TO COMPONENTS OF A PATIENT'S ELECTRONIC CASENOTE

A patient's electronic casenote includes all information (both clerical and clinical) collected or entered about a patient, including demographic details; address history; District Health Authority (DHA) history; general practitioner (GP) history; aliases; unit numbers; episodes; events; results; people and teams; casenote movements; medications; diagnoses; procedures; alerts; clinical proformas; letters; Mental Health Act details; treatment plan; dependency scores; care plans; etc.

However, individual users of the CIS may only be given rights to see the parts of the total patient record that are relevant to their needs as clinicians, administrators, and so on. That is, each individual user (or more often group of users) can be provided with an electronic casenote that is tailored according to the nature and the needs of their job (and the patient information they need to have access to in order to perform that job appropriately).

Additionally, for any item to be included in a user's electronic casenote, it is also possible to assign 'read-only rights', which means that patient data may be viewed but not amended or added to.

Here are some examples of electronic casenotes tailored to the needs of individual users:

- out-patients receptionist – demographic details; unit numbers; DHA history; episodes and events; casenote movements.
- ward nurse – demographic details; people and teams; diagnoses (read and write); medications (read only); results (read only); observations (read and write); treatment plan; care plans; dependency scores.
- consultant (mental health) – demographic details; people and teams; diagnoses (read and write); medications (read and write); results (read only); psychiatric assess-

ments; treatment plan; previous clinical letters; Mental Health Act status; appeals and tribunals; care programme approach plans.

RESTRICTED GROUPS

A formal approach has also been taken to the problems that arise when certain elements of a patient's clinical record may be deemed to be sensitive.

The system has the facility to set additional confidentiality flags on specific records, such as medications, diagnoses, clinic attendances and letters. This is useful for areas such as *in vitro* fertilization (IVF), child and adolescent psychiatry, and some genitourinary activity.

The confidentiality level may be set to either:

- any authorized user; or
- restricted groups.

Note that records marked as restricted will be completely invisible to unauthorized users. As an example, an individual consultant's psychiatric correspondence may be marked as restricted and only the author, recipient and typist are aware of the letter and its contents.

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 marking certain clinic appointments as restricted is that a user from one specialty would be able to book an out-patient appointment at the same time as a planned confidential visit to another specialty. The problem with marking certain medications as restricted is the obvious one of hiding a dangerous drug interaction. We have not resolved this but one solution is to use the system to advise of a drug interaction without identifying the relevant drug, leaving it to the clinician to then discuss this directly with the patient.

In practice, we do not encourage users to set additional confidentiality flags on information unless absolutely necessary.

CLINICAL AUDIT AND AGGREGATED INFORMATION

The requirement for patient confidentiality at some point comes into conflict with the need to share clinical information for education or for healthcare planning. This is well understood by clinicians in the field of clinical audit. This requires the aggregation of personal health information and, indeed, the aggregation of clinician-based information.

Two approaches are being taken to this:

1. Where a clinician considers that there will be benefit in gaining access to a patient's electronic casenote, an identified audit enquiry can be made, in which case the system will only list patients to whom she has access. This may be particularly useful where an audit enquiry requires a detailed clinical examination of the circumstances surrounding a particular case and, therefore, requires access to the electronic casenote.
2. Where crude population-based information is all that is required, unidentified statistics can be extracted.

This approach does not satisfy the requirements of Korner returns or indeed the statutory obligation placed upon NHS Trusts to supply identified information to Cancer Registries. There is conflict here that will need to be resolved.

IMPLEMENTING CONFIDENTIALITY CONTROLS

The system uses objects and properties to set up a wide range of parameters used to control how the system operates, including controlling access to patients and information about them. Properties can be attached to objects representing many different parts of the system at various hierarchical levels. For example, properties can be attached to users, or groups of users. System level properties are also used for a number of system-wide controls mechanisms (e.g. whether confidentiality controls are 'on' or 'off').

Properties may be either unique or additive:

- Unique properties are destructive, in that setting a unique property replaces any previous setting for that property. Thus, if access to a patient's diagnoses is set to 'Read-only' for a group to which the user is a member, but an individual user property is set to 'Edit allowed', the individual property will supersede the group property.
- Additive properties are non-destructive, and superimpose themselves on one another. Data access rights are an example where a user with two jobs may be given access to out-patient data for one specialty in their capacity as a clinic clerk, and to Accident and Emergency Department

Table 1 Properties used to implement confidentiality controls within the CIS

System property	Description
Confidentiality activated	Activates confidentiality checks (i.e. without this property present, all users have access to all patient records without restriction, regardless of whether other confidentiality properties have been assigned).
Confidentiality expiry period	The number of days' interval between recording patient accesses (if this property is not set, the default is 1, i.e. a daily check).
User/group property	**Description**
Rights: no restriction	Allows the user/group unrestricted access to all parts of all patients' records.
Rights: override allowed	Allows the user/group to override confidentiality restrictions.
Rights: CIS – list types	Limits access to patients on one or more types of lists (e.g. in-patients, recent in-patients, discharge summaries, clinical coding, etc.).
Rights: CIS – wards	Limits access to patients who are or have recently been on the selected ward/s.
Rights: CIS – specialties	Limits access to patients who are or have recently been under the care of the selected specialty (specialties).
Rights: CIS – clinicians	Limits access to patients who are or have recently been under the care of the selected consultant(s).
Rights: restricted groups	Allocates the user/group to specific restricted groups (e.g. IVF, HIV, mental health, child and adolescent psychiatry etc.).
Rights: CIS – electronic casenote	Limits access to selected electronic casenote options. Multiple tick-box selection of electronic casenote options.
Rights: CIS – read only	Restricts access to selected clinical items (e.g. diagnoses, procedures, medications, etc.) to read only (i.e. prevents user from updating items). Multiple tick-box selection of electronic easenote options.

Abbreviations: CIS, clinical information system; IVF, *in vitro* fertilization; HIV, human immunodeficiency virus.

(AED) records in their capacity as an AED clerk. Being made a member of the AED group adds to existing rights rather than replacing them.

Table 1 summarizes the properties relevant to protecting the confidentiality of patient information within the CIS, with a short description of their effect.

During the set-up of user groups (e.g. nurses on a particular ward, consultants within a particular specialty, secretaries working for a particular consultant, and so on), consideration needs to be given to the combination of confidentiality rights that are required for the users to carry out their daily activities, without compromising the confidentiality of patient information.

Practically speaking, the set up of appropriate confidentiality rights is a non-trivial task that involves balancing of sometimes conflicting concerns. For example, in principle, it might be thought appropriate to limit the access of rights of ward nurses to the ward(s) that they work on. In practice, this might prove difficult given the unpredictable nature of which wards a nurse might be called to work upon (particularly at night). This problem might be resolved by giving nurses ward rights to the wards they most often work on but supplementing these rights with a confidentiality override, and monitoring the number and nature of such overrides.

USERS' EXPERIENCE

This formal approach to the confidentiality of patient information has been progressively implemented over the last five years. Initial responses from users were along the lines of 'What's all this cloak and dagger stuff?' As users have become aware of the depth and breadth of information that is immediately available on their patients and also on themselves and their relatives, this view has altered. There is now a clear recognition of the importance of these measures.

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, at Hastings there has not yet, in five years, been a single request by a patient for such a report.

CONCLUSION

A practical approach to managing the confidentiality of patient information in large scale clinical information systems in the acute hospital has been described. The traditional approach of limiting the functions that hospital staff can undertake is necessary but not sufficient. Control over access to the individual patient is required, with this access only being granted when the member of staff's rights match a patient's current clinical contacts. In our experience, the setting-up and maintenance of such rights is a non-trivial, but achievable task.

References

[1] Burns F. Information for Health. NHS Executive, 1998.

[2] Anderson R J. *Security in Clinical Information Systems*. London: BMA, 1996.