

A proposed framework for a secure Health Information System

Research Report



**prepared by
Kim Hagen-Hall**

for 157.733 Health Information Systems

Abstract

Maintaining security, privacy and confidentiality of healthcare information is of great importance in keeping patients' confidence in the healthcare system. This report proposes a framework for implementing security in a Healthcare Information System incorporating role-based access to database tables and allowing specific records to be flagged as confidential.

The implementation of a prototype system is described. The framework was implemented successfully and provides for access to critical information through the use of an audited "override" feature, ensuring that patient care will not be compromised. Example business rules are applied to the system and possible future extensions to the framework are discussed.

1. Introduction

Maintaining security, privacy and confidentiality of healthcare information is "of great importance in keeping patients' confidence in the healthcare system" (Van de Velde & Degoulet, 2003). Healthcare organisations have responsibilities under the Privacy Act 1993 and the Health Information Privacy Code 1994 to keep patient information private and secure. The potentially huge cost of a privacy breach (Willams, n.d.), and the resulting political and media pressure, make the possibility of a privacy breach almost unthinkable. Many sources recommend that health information systems allow access only to the information that a staff member needs to know to effectively do their job (Gillespie, 2007; Win et al., 2006; Van de Velde & Degoulet, 2003; Bakker, 2002; Denley & Weston Smith, 1999).

This report investigates how this could be achieved without compromising patient care. The questions asked are:

1. what security measures are recommended by the literature;
 2. can these measure be implemented "workably" in a Health Information System; and
 3. when implemented, can these measures allow access to the information that healthcare workers need to see?
-

2. Literature Review

2.1. Information needed by healthcare workers

Healthcare Information Systems support patient care, quality assurance, research, epidemiology and administration functions within healthcare organisation (Hovenga, Kidd & Cesnik, 1996). The core of these functions is often an ADT (Admission, Discharge and Transfer) system (Hasset, 2002) which "collects, stores and tracks patient information from admission to discharge" and this data facilitates functions such as bed control and patient census records (Hasset, 2002). All patient care and treatment interactions are tracked or linked to this basic information (Hasset, 2002), and the system may interface with results reporting systems which

report individual test results, speciality support systems such as radiology, laboratory or pharmacy systems, and order entry and financial reporting systems (Hasset, 2002).

Patient data stored may include information containing name, address, occupation, marital status, current health status, medical history, progress notes, referral letters, prescription charts and laboratory reports (Engelbrecht, 2003); demographics, insurance information, medical record number, care provider and next of kin (Hasset, 2002); date of birth and documentation of each care event, including symptoms diagnosis, treatment and outcome (New Zealand Health Information Service, 1997). Relevant documents and correspondence from external organisations such as physiotherapists, radiologists and medical laboratories may be included, and often arrive in hard copy form (New Zealand Health Information Service, 1997).

Healthcare professionals desiring access to patient information General Practitioners (GPs) and practice nurses, secondary care providers such as critical care unit and intensive care unit personnel, attending physicians, consulting specialists, ward nurses, emergency responders and other primary healthcare providers such as physiotherapists and community health workers.

There do not seem to have been many studies that identify the information that particular healthcare workers need to access. In studying the information needs of GPs, Engelbrecht (2003) found that GPs accessed the following information from medical records during consultations:

- patient history
- practice nurse/receptionist communications,
- secondary care discharge summaries
- communications from other health professionals
- community health care workers info
- pathology, radiology and other test results,
- NHI information
- ACC information

Given the lack of studies in this area, a healthcare organisation implementing security features would need to conduct a careful study into the information that groups of staff members need to have access to, in order to ensure that they are not denied access to critical information.

In addition to information needs, Healthcare organisations have unique environmental factors that must be taken into account.

2.2. Environmental Issues in a healthcare setting

Access to information in a General Practice clinic can be controlled fairly simply: only a few people have access to the information system at all, and the personal nature of the relationships hopefully encourages professional practice by those people.

However in hospitals the following issues arise:

- a large number of employees makes access management difficult (Gillespie, 2007);
- nurses' and junior doctors' roles change frequently and quickly at (Williams, n.d.);
- in critical care and intensive care units each clinician needs immediate access to vital patient information to effectively provide patient care, and access to health information needs to be controlled without disrupting the clinical workflow (Gillespie, 2007);
- there are few clear divisions of responsibility; access to patients' data could reasonably be seen as necessary for most health professionals for most patients they are treating (Williams, n.d.), and the teams responsible for a particular patient's care change quickly (Denley & Weston Smith, 1999); and
- in healthcare organisations patients and the general public are "almost everywhere", allowing them to see computer screens (Williams, n.d.) or printed reports inadvertently.

These factors make implementing security measures more difficult than in many other types of organisations.

2.3. Possible security measures

Access to healthcare information systems is typically restricted to the use of individual logins (Van de Velde & Degoulet, 2003). Older systems allowed valid users to see almost all data (Gardner, 1999), but more modern systems allow access only to particular data sets, based on criteria such as:

- relation to the patient (Bakker, 2002) – e.g. their GP or current care team;
- role (Van de Velde & Degoulet, 2003; Bakker, 2002; Gillespie, 2007) – e.g. occupational group or seniority;
- timeframe (Van de Velde & Degoulet, 2003) – e.g. a specialist for a consultation, a nurse for a shift;
- location – which workstations a particular role can use to access information (Van de Velde & Degoulet, 2003); or
- specific criteria – e.g. patient consent or an emergency (Van de Velde & Degoulet, 2003).

Information may be divided into subsets, by marking specific information (e.g. psychiatric reports) as confidential (Denley & Weston Smith, 1999) or splitting personal and clinical information (Van de Velde & Degoulet, 2003), with different roles having access to different levels of information.

In addition, access to data can be logged based on user name, role, date or time (Denley & Weston Smith, 1999), with logs audited to detect misuse.

2.4. Essential considerations

In selecting an appropriate combination of security measures, the following must be considered:

- Each member of the clinical workforce needs immediate access to vital patient information (Gillespie, 2007);
- patient care must not be compromised; and
- solutions need to be socially acceptable, practical and affordable (O’Conor, 1999).

An “override” feature is necessary to ensure that access to critical data is not denied. While this could be misused (Bakker, 2002), Denley and Weston Smith (1999) found that notifying the user that access will be logged and reviewed “effectively deters misuse”.

Logging on to the system must be quick. Typing user names and passwords is slow – barcodes on staff cards and fingerprint scanners are now mature and very quick, but login procedures must also perform only necessary functions (for example, a full Windows XP login would be too slow).

Denley and Weston Smith (1999) note that showing only subsets of information – for example hiding psychiatric information – leads to problems identifying drug interactions, as clinicians may not see all a patient’s prescribed drugs. They have not found a solution to this problem.

2.5. Additional measures

Technical measures alone are not enough: security can still be compromised through the actions of properly authorised personnel. Supporting organisational measures are needed, such as preventing unauthorised or inadvertent access to printouts (Bakker, 2002) and computer screens (Williams, n.d.), educating staff on the importance of privacy, and setting rules for using patient data for research, such as requiring explicit consent (Bakker, 2002).

3. Methodology

An action research methodology was used to put the literature discussed above into a practical framework. The following steps were taken:

- a demonstration healthcare information system was designed based on the information needs identified in the literature;
- a reasonable subset of the security options identified from the literature was chosen for implementation;
- a security system was designed based on the information needs identified and the chosen security options, and a prototype system developed; and
- the prototype system was evaluated against the information needs identified and potential business rules for data access.

4. The Healthcare Security Prototype

The prototype implemented consists of a demonstration patient information module and an overlying security framework.

4.1. The Patient Information Module

The patient information module demonstrates how the security measures would work in practice. The module displays the following information:



- Patient information: name, address, occupation, marital status, demographics and ethnicity information, as shown in figure 1; and
- Care Event History, as shown in figure 2. For each care event symptoms, outcomes, consultation notes are shown on the main screen, with treatments, referral letters, prescriptions, tests ordered and test results shown on child screens.

Figure 1: The patient contact and demographic information screens

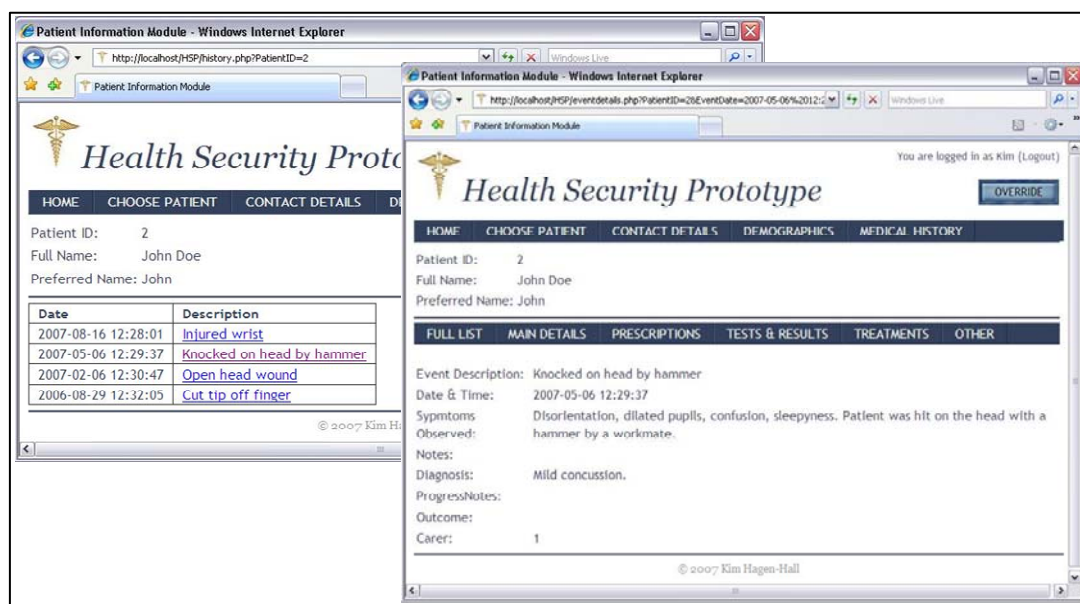


Figure 2: The care event history and details screens

The underlying data model is shown in figure 3. The demonstration system currently only displays data; update features could be added in later versions. The security module was then created as a layer over this system.

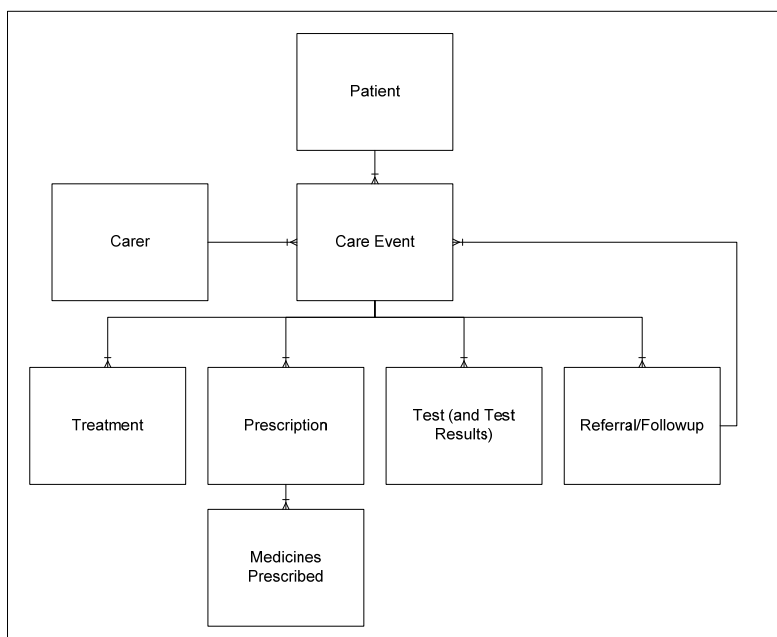


Figure 3: the patient information system data model

4.2. The Security Framework

The following security features were implemented:

1. Limit data access based on staff roles (Van de Velde & Degoulet, 2003; Bakker, 2002; Gillespie, 2007) which are time-based (Van de Velde & Degoulet, 2003);
2. restrict access to database tables;
3. subset data (Van de Velde & Degoulet, 2003);
4. allow records to be “flagged” as confidential (Denley and Weston Smith, 1999); and
5. have an “override” function to allow critical access (Denley and Weston Smith, 1999).

The database model for the security module is shown in figure 4. The tables with dashed lines were not implemented due to time limitations.

The pivotal table is the Role table. Users are assigned to roles as shown in figure 5, such as a GP or a Practice Nurse role. Roles are given permission to see specific database tables and

specific flags, as shown in figures 6 and 7.

4.2.1. User Roles

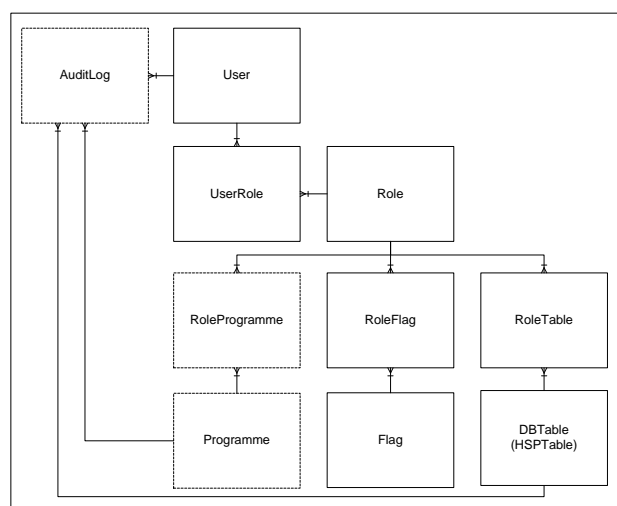


Figure 4: the security framework data model

A user may have more than one role. As shown in figure 5, Roles may have a start and/or end date & time. This allows a user to have a role only for a specific time period, or after or until a specific date and time. This also allows roles to be set up in advance, for example by a staff scheduling system. This would reduce the problems experienced by Gillespie (2007) who found that updating user permissions was taking up to three months.

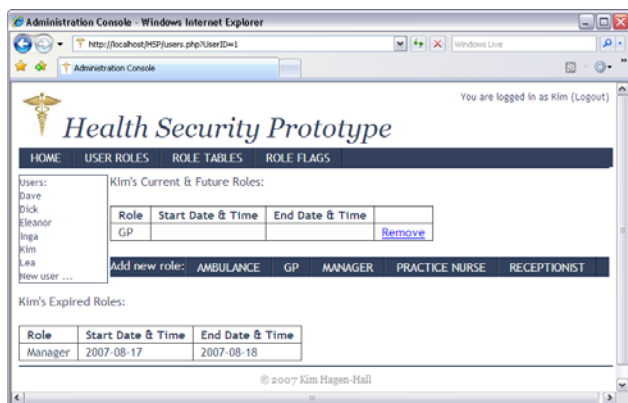


Figure 5: Role assignment

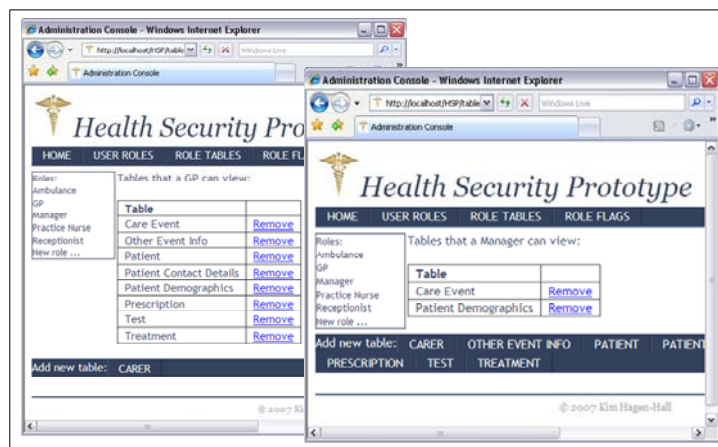


Figure 6: Table access set up for GPs & Managers respectively

role which has been given access to the relevant table(s). Figure 6 shows the table access rights set up in the demonstration system for GPs and managers respectively.

This is used in conjunction with **data subsetting** to provide access to only the data that a user should see. Data Subsetting – moving some data into another table – was suggested by Van de Velde & Degoulet (2003), and was used to restrict access to patient contact details and demographics, which were

moved to separate database tables. The results of this are discussed in section 4.2.6. In database management systems which support Table Views, such as Oracle, the data could be kept in the same table and the system could give permissions to views rather than tables.

However both of these solutions require some customisation by developers – the developers must move the fields to a new table or alter the views, and alter the programme code to access the new tables or views.

4.2.3. Flags

Flags are user-customisable, and therefore cheaper to implement. Users can add new Flags to the database – for example “GP Only” or “Confidential” – and roles are given access to these flags, as shown in figure 7. All tables in the patient information module have a “flag” field. If a flag is entered into



Figure 7: Flag access for GPs and managers respectively

this field, users will only be able to see the record if they have a current role which has access to that flag.

4.2.4. Override

The Override feature is essential to allow access to critical data. It has been implemented so that it is only active for the current screen - if the user goes to another screen they must invoke the “override” feature again.

In future versions the following information would be logged: user name, date & time, the data accessed, and a flag to say that the “override” feature was being used for this access. This information would be sent to an appropriate manager for review, as done by Denley & Weston Smith (1999). These features have not yet been implemented due to time constraints.

4.2.5. The Data Retrieval Query

Access to tables and flags was checked with a generic SQL query shown in figure 8. It is shown here to prove how simply the system can be implemented. The query selects the data requested only if:

- The user has pressed ‘override’
- OR
- The user has a current role which has permission to view the table,
- AND
- Either there is no flag, OR the user has a current role which has permission to view that flag.

```
SELECT * FROM $Table
WHERE $WhereClause

AND (('Override' <> '') /*either the user has pressed 'override' */

OR /*or they have permission to see the table*/
(
  EXISTS (SELECT * FROM userrole, roletable
  WHERE userrole.UserID = '$UserID'
  AND (ISNULL(userrole.StartDate) OR userrole.StartDate <= now() )
  AND (ISNULL(userrole.EndDate) OR userrole.EndDate > now() )
  AND userrole.RoleID = roletable.RoleID
  AND roletable.TableName = '$Table')

  AND /*and there is no flag, ...*/

  (ISNULL($Table.FlagID)

  OR /*...or they have permission to see the flag*/

  EXISTS (SELECT * from userrole, roleflag
  WHERE userrole.UserID = '$UserID'
  AND (ISNULL(userrole.StartDate) OR userrole.StartDate <= now() )
  AND (ISNULL(userrole.EndDate) OR userrole.EndDate > now() )
  AND userrole.RoleID = roleflag.RoleID
  AND roleflag.FlagID = $Table.FlagID))
)
)
```

Figure 8: the standard data retrieval query

The Override variable, \$Override, is set to blank when the user opens a screen. The Override button, which can be seen in figure 9, sets the “override” variable to “True”.

This query is fairly simple, and easily put into a generic stored procedure called by all screens, simplifying support and maintenance.

4.2.6. The Security Framework in action

In the demonstration system, the Patient table was divided into subsets – patient information (name and NHI number), contact information and demographics. The following permissions were set up:

- GPs were given access to all tables and to the flags “GP Only” and “Confidential”.
- Receptionists were given access to patient information and contact details, but nothing else.
- Practice Nurses were given access to patient information and demographics, but not contact information.
- Managers were given access to demographics and care event history, but neither patient information nor contact details.
- Ambulance crew were given access to patient information, demographics and care event history, but not to any flags.

As seen in figure 9, a practice nurse can see the demographic information, but the receptionist does not. The manager sees the demographic information but not the name of the patient to whom it refers.



Figure 9: Demographic information as shown to a practice nurse, receptionist & manager, respectively

If the user does not have access to the information, they see “Restricted” in place of the information. This warns them that data is there, but not available with their current level of access. While this might incite curiosity (Bakker, 2002), there are cases where this is important, such as drug interactions (Denley & Weston Smith, 1999). If

you can see that there is a prescription there, then you can get access to it if the patient is not conscious.

If the example receptionist, Eleanor, was to override the security, a warning message would be displayed and the unrestricted information would be shown on the screen, as seen in figure 10. The override feature is only active on the current screen – if the user moves to another screen or chooses another patient they must click “Override” again.

Finally, in John Doe’s medical record, one care event was marked as “GP only”. When a GP accesses the care event history, all information is shown. However when an Ambulance crew member accesses the care event history, the flagged record is not shown.

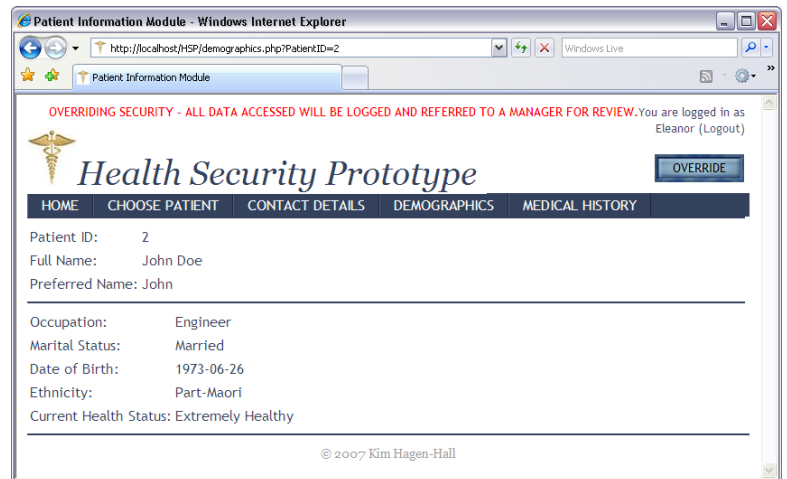


Figure 10: the override feature in action

5. Findings

The security framework was implemented successfully, allowing access to be restricted vertically (by table) and horizontally (by flag), and this was able to be refined into a fairly simple solution.

The implementation demonstrated both “restrictive” and “permissive” and restrictions – database tables are not shown unless you have permission (“restrictive”) but rows are shown unless they are flagged (“permissive”). Either model could therefore be implemented using this framework.

The essential considerations identified in section 2.4 were generally included:

- Each member of the clinical workforce can have immediate access to vital patient information;
- patient care should not be compromised; and
- it is felt that the solution would be socially acceptable, practical and affordable.

As discussed in section 4.2.2, subsetting of data may be expensive if the organisation wishes to restrict data access in non-typical ways. While it would be possible to extend the proposed framework to restrict access by field as well as table, the solution would be far more complex; it would be harder to get permissions right, leading to delays and errors, and the data retrieval queries would be more complex, leading to slower performance and more bugs.

5.1. Business Rules applied to the framework

The following example business rules demonstrate the sorts of rules that can be implemented using this framework:

- GPs can have access to all tables, “GP only” flags but not “Patient Consent needed” flags;
- Practice nurses can have access to patient information & demographics, but not contact information;
- Ambulance crew can have access to patient care events, treatments, prescriptions and tests, but not if they are flagged;
- Receptionists can have access to patient contact details, but nothing else;
- Administrators can have access to patient demographics, but not patient contact details or care events;
- People may have access after or before a certain date, or between certain times;
- Lea will have the “practice nurse” role from 14:00 on date x to 23:00 on date x, and 05:00 on date y to 14:00 on date y; and
- Elizabeth will have the GP role from 4/10/2007 to 20/10/2007 (e.g. for locums working for 2 weeks).

The following business rules cannot be implemented in the current framework:

- Ambulance crew can have access to all current medications/all medications prescribed in the last year/all care events in the last 2 years;
- Emergency department staff can have access to all medical information in the past 2 years;
- Ward nurses can have access to all information related to the current care event only; and
- Lab technicians can have access to lab tests and results for a specific patient, but not all patients.

If organisations want to implement these sorts of rules, the following additional functionality would need to be added:

- access to information based on the date of the information – e.g. in the last year, 5 years etc.
- access to specific care events – e.g. ones for which your team is currently responsible; and
- access to specific patients – e.g. patients for which you are currently responsible.

This functionality would, of course, increase the complexity of the solution, making it harder to manage and maintain, and reducing system response times.

5.2. Organisational measures

In addition to technical measures, organisational measures must be put in place to ensure that “people errors” do not arise. While this is a matter outside the scope of the current study, the following measures were identified during this study:

1. User permissions must be updated in a timely manner: this should be automated as far as possible and managers will need to employ enough staff to manage permission changes quickly (Gillespie, 2007).

2. Regular checks need to be made to ensure that permissions are suitable and allow access to needed data. Poor practices such as sharing logins are signs that permissions may be too restrictive.

3. All staff need to ensure that unauthorised users do not gain inadvertent access to information, such as through printouts or unattended computer screens.

4. All staff members need to be aware of the importance of privacy and confidentiality in healthcare organisations, and know not to provide access to others without reason or share passwords.

6. Conclusion

The framework was successfully implemented in a fairly simple way, which indicates its potential if it meets the needs of healthcare organisations. The override feature allows access to critical patient information without compromising patient care, while retaining control by monitoring how it is used.

Little academic research has been done to date to identify the information needs of different healthcare workers; this is a useful area for future study and would further inform the validation of the proposed framework. While the framework could be extended, for example to allow access only to current care teams, this would increase the complexity, and therefore the time needed to manage and maintain the system, so a real need must be demonstrated for this functionality.

Further work is needed to analyse methods for authenticating users quickly, for example using fingerprint or barcode scanners, and in a production system role setup would need to be automated, for example by a link to a staff scheduling system. Future prototypes would include auditing of data access and would extend the framework to include data updates as well as retrieval.

References

- Bakker, A. (2002) Data Protection and Confidentiality. In J. Mantas and A. Hasman (Eds.), *Textbook in Health Informatics* (pp. 450-464). Amsterdam: IOS Press.
- Denley, I. & Weston Smith, S. (1999). Privacy in clinical information systems in secondary care. *British Medical Journal*, 318, 1328 – 1330.
- Engelbrecht, J. (2003). *Evaluation of IS support for the clinical decision making process in Primary Care* [Unpublished report]. Palmerston North: Massey University: Department of Information Systems.
- Gardner, M. (1999) Commentary: Let's discuss wider social and professional issues [Commentary to Denley, I. and Weston Smith, S. (1999). Privacy in clinical information systems in secondary care. *British Medical Journal*, 318, 1328 – 1330] *British Medical Journal*, 318, 1330 – 31.
- Gillespie, W. (2007) The keys to the kingdom. *Health Management Technology*, 28(3), pp34-5.
- Hasset, M. (2002). *Applications for Health Care Information Systems*. In Engelardt, S. and Nelson, R. (Eds.) *Health Care Informatics*. Mosby: St Louis pp147-160.
- Hovenga, E., Kidd, M and Cesnik, B. (1996). *Health Informatics: An overview*. Churchill Livingstone.

New Zealand Health Information Service (1997). Electronic Medical Records. Retrieved 15 January, 1997 from www.health.govt.nz/NZHIS/EMR.html.

O'Connor, R. (1999) Commentary: Organisational and cultural aspects are also Important [Commentary to Denley, I. and Weston Smith, S. (1999). Privacy in clinical information systems in secondary care. *British Medical Journal*, 318, 1328 – 1330] *British Medical Journal*, 318, 1331.

Van de Velde, R. and Degoulet, P. (2003). *Clinical Information Systems: A component-based approach*. New York: Springer.

Williams, L. (n.d.). *Health Information and Privacy at Auckland Healthcare* [Handout]. Palmerston North, New Zealand: Massey University: Postgraduate Diploma in Business Administration: 157.733 Health Information Systems.

Win, K. T., Susilo, W. and Mu, Y. (2006). Personal Health Record Systems and Their Security Protection. *Journal of Medical Systems*, 30, 309 – 315.