HIC 2008 Australia's Health Informatics Conference
Editor: Heather Grain
Publisher: Health Informatics Society of Australia Ltd (HISA)
ISBN 978 0 9805520 0 3 ©The author(s) & HISA All rights reserved

EHR Privacy Risk Assessment Using Qualitative Methods

Maria Madsen

Central Queensland University, Gladstone, Queensland

Abstract

Objective: The objective of this investigation was to produce a taxonomy of privacy risks to assess the risks associated with Personal Electronic Health Records (PEHR) and Centralized Electronic Health Records (CEHR) based on key threats. **Background:** Privacy and security risks are intrinsically connected. Both internal and external security threats put patient privacy at risk that require both technological and human controls. **Methods:** National Hospital Morbidity Data (NHMD) reporting was chosen as the CER use context for the risk assessments. Cultural Historical Activity Theory (CHAT), was used to identify and analyse privacy risks. A qualitative risk assessment approach was adopted. **Results:** A privacy risk management tool (PRMT) was developed from the risk assessment process. The PRMT was used to analyse privacy risks associated with morbidity data reporting and the use of patient held health records as an example of a PEHR implementation. **Implications:** The examination of the NHMD highlighted risks associated with secondary and tertiary uses of patient data. The examination of the use of a personal electronic health record in the context of morbidity data reporting suggested that the introduction of multiple copies of the patient record was likely to increase the risks to data integrity and re-identification of the individual, and subsequently increase the risk management cost.

Keywords:

Qualitative Risk Assessment, Information Privacy, EHR, Security Behaviour, Risk Treatment

Objective:

The objective of this investigation was to produce a taxonomy of privacy risks to assess the risks associated with electronic health records stored centrally and those stored by the individuals themselves. The taxonomy developed into a risk management tool that may be used to guide and facilitate privacy risk assessment of health care systems.

Background:

Electronic health records pose risks to patient privacy that are not found when paper-based records are used. Even when patient data is used in accordance with the Privacy Act 1988 (Cth), patient privacy may be compromised because health care organizations are allowed to collect and share sensitive patient information without acquiring consent and without de-identifying the data if it is impracticable. Legal uncertainties such as this and the changing nature of EHR implementations threaten patient privacy and trust.

> "… people will only gain the benefits of EHRs if they trust the system – and that means getting the privacy and security issues right. … It is the job of people designing EHR systems to minimise these risks as much as possible – by using the best technology, legal safeguards, policies, procedures, and training", (APF 2006).

Any examination of information privacy must necessarily involve an examination of information security because the objectives and tasks of these two functions are inextricably linked. To date, much information security research focuses on threats that are external to the organization. Internal threats are less commonly examined even though statistics suggest that threats from internal sources are perhaps more common than those from external sources (Stanton et al. 2005). Privacy and security research tends to report security management through new technologies. Likewise much of the money spent on systems security is spent on technological solutions. Unfortunately, even the most sophisticated technological solution can be undermined by poor security behaviour. Stanton et al. (2005) have categorized information security behaviours in terms of the level of expertise required and the intentionality of the behaviour, Figure 1.

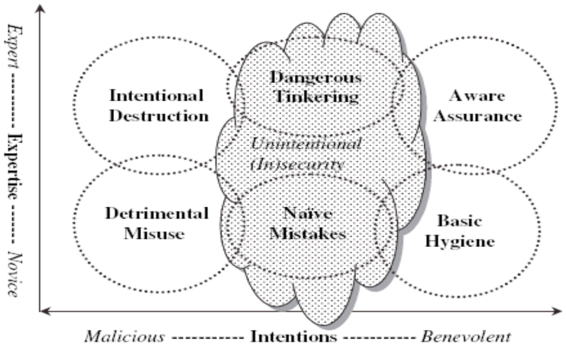
Expert ------- Expertise ------ Novice
Intentional Destruction
Dangerous Tinkering
Aware Assurance
Unintentional (In)security
Detrimental Misuse
Naive Mistakes
Basic Hygiene
Malicious ---------- Intentions ---------- Benevolent

Figure 1. *Two-factor taxonomy of end user security behaviours.*

Figure 1 Taxonomy of End User Security Behaviors (Stanton et al. 2005)

The area identified as Unintentional (In)security, above, presents an almost certain source of risk. The consequences from actions and activities that fall within this type of behaviour will vary from minor to extreme. For example, a password on a sticky note in a staff only area may have only minor consequences while a lost thumb drive housing an entire data set, the NHMD for example, may have major legal and financial consequences for both the patients and the business.

Methods:

The national hospital morbidity data set (NHMD) was chosen as a context for this risk assessment because it exemplifies a secondary mandatory use of health data. The NHMD is an aggregation of de-identified data collected nationally. The NHMD is specified by the Australian Institute of Health and Welfare (AIHW) at a national level, but individual states may and do modify data item names and may require submission of additional information. The content of the data set has changed on an annual basis since the inception of the collection in 1987. The current NHMD contains data elements in the following groups: Establishment data, Demographic data, Administrative data, Length of stay data, and Clinical and related data (AIHW 2006). There are no data elements that can be used to directly identify any individual patient. In itself then, this set of data appears to present a low risk to patient privacy.

Cultural Historical Activity Theory (CHAT) was used to describe the risk context, i.e. to identify and analyse the risks. Figure 2 shows the generic elements of an activity.

Activity Name	**Subject**	**Object**	**Rules**	**Community**	**Tools**	**Division of Labour**	**Intended Outcome**
Name the activity	Who is doing the work?	What or who is being worked on?	What rules apply? Rules may be internal or external.	What groups are involved or have a stake in this activity?	What tools, are used? Includes ideas or conceptual models.	How is work distributed? What roles are essential?	What need is satisfied? What outcomes are produced?

Figure 2. *Elements of an activity in Cultural Historical Activity Theory*

CHAT fundamentally focuses on the person doing the activity. All other elements are seen as mediators of the work. The activities of interest here include morbidity data collection, morbidity data exchange, and EHR privacy protection.

The risk assessment was framed within the risk management context of Australian information security standards including HB 231:2004 (SAI 2004) , HB174:2003 (SAI 2003). and HB167:2006 (SAI 2006). In brief, information security standards recommend that risks are identified, analysed, evaluated, and treatment options recommended. A qualitative risk assessment is an estimated probability of risk based on the likelihood of an identified threat occurring and the severity of the consequences if it does. The general evaluation criteria are categorised in Figure 1 below.

Risk Level	**Likelihood**	**Severity**	**Consequences**
Low	Unlikely to Almost Certain	Minor	**Minimal impact** to the patient or business.
Moderate	Possible to Likely	Moderate to Critical/Extreme	**Moderate impact** - moderate to major loss of reputation, patient confidence, or embarrassment or loss of income.
High	Likely to Almost Certain	High to Critical/Extreme	**Major impact** - perhaps by major loss of reputation, patient confidence, [identity theft], or embarrassment or loss of income. It may even be life threatening. Recovery may take an extended period of time.

Figure 3. *Evaluation Criteria Categories (adapted from HB 231:2004, p. 80).*

Treatment options range from Risk avoidance to Risk retention (SAI HB 231:2004, pp.17-31). The most usual risk treatments are those that reduce the likelihood or reduce the consequences of an event. The Australian Computer Crime and Security Survey (AusCert and ALEA 2006) reported the security technologies and policies most commonly used by Australian organizations. These are categorized by risk treatment type in Table 1.

Treatment Type	Technology Treatments (Barrier Controls)	Policy Treatments (Behavioural Controls)
Risk avoidance	Disconnect from network and/or internet	Decommissioning equipment procedure
Likelihood reduction	anti-spam filters, anti-virus software, digital identifiers or certificates, virtual private networks, encrypted logins and sessions, encrypted files, firewalls, biometrics, smart cards, one time tokens, reusable passwords, and access control	cryptographic controls policies or procedures; external network access control policies; user responsibility policies; segregation of duties policy; change control procedures; and documented standard operating procedures; controls against malicious software
Consequence reduction	intrusion detection systems, file integrity assessment tools	system audit policy; monitoring system access and use procedures;
Risk transference	Not applicable	Insure against potential risks; Outsource or contract with 3rd party that has the technology that you need, [for example using a certificate authority for key management in a PKI system]
Risk retention	Too costly or not available	business continuity management, incident management procedures; forensic plan

Table 1. *Information security risk treatments*

The Privacy Risk Management Tool:

EHR security and privacy issues identified by the APF (2006), security behaviour types (Stanton et al. 2005), the Privacy Act 1988 (Cth), the traffic light approach (WHS Qld 2007), and the methods discussed above have informed the development of a privacy risk management tool (PRMT), Figure 4. To achieve a reasonable level of risk control the answer to each of the risk assessment questions should be, "yes".

Risk Factor	**High Risk** **Very Likely to Cause Privacy Breach (*Red*)**	**Moderate Risk** **Some risk of breach &** **Short term controls (*Amber*)**	**Low Risk** **Less likely to result in privacy breach & possible controls (*Green*)**	**Risk Assessment Questions (Yes/No)**
External access to EHR system	× Minimal or missing access controls (eg. password only identity verification with poor password hygiene) × Inadequate network and/or internet security × Insufficient security training and education of users including personnel and patients × Encryption is not used for email	≈ Basic access control in use (eg. password only with good password hygiene) ≈ Basic network and internet security protocols used ≈ Infrequent monitoring of system access	✓ Strong access controls in use ✓ Encryption is used ✓ Users are informed and trained. ✓ Internet & network security protocols in use ✓ Data integrity checking is used ✓ Virtual Private Network in use ✓ System audits and access monitoring active	1. Are data transmissions encrypted? 2. Are users educated about the risks involved in accessing EHR using the internet? 3. Are users trained to use the system? 4. Is the system robust against user error? 5. Are people given the option to opt out of using the system? 6. Is connection secure end to end?
Internal access to EHR system	× Minimal or missing access controls (eg. password only identity verification with poor password hygiene) × Insufficient security training and education of personnel × Encryption is not used for email × Failure to limit use of EHR (eg. records can be copied to removable media and taken off site)	≈ Basic access control in use (eg. password only with good password hygiene) ≈ Basic network and intranet security protocols used ≈ Security behaviour policies exist but explicit training not provided	✓ Strong access controls in use ✓ Encryption is used ✓ Users are informed and trained. ✓ Internet & network security protocols in use ✓ Data integrity checking is used ✓ Virtual Private Network in use ✓ System audits and access monitoring active	1. Is data access tracked via a system log? 2. Is the access log checked on a regular basis for anomalies or exceptions? 3. Are staff properly informed about their ethical, moral, and legal responsibilities? 4. Is the system designed to alert security mangers about unauthorized access and/or use of data records?
Personal EHR on removable media	× Minimal or missing access controls (eg. password only identity verification with poor password hygiene) × Inadequate network and/or internet security × Insufficient security training and education of patients × No synchronization of PEHR with master copies	≈ Basic access control in use (eg. password only with good password hygiene) ≈ Basic network and internet security protocols used ≈ Intermittent synchronization (eg. only on manual request)	✓ Access Controls are in use ✓ Data is encrypted ✓ Users are informed about how to use the system. ✓ Error checking on data entry ✓ Internet security protocols are in use ✓ Data integrity checking is active & synchronization of copies is automatic.	1. Are people given the option to opt out of using the system? 2. Is the PEHR encrypted? 3. Are access controls used for both portable EHR and system? 4. Is the patient able to access and correct personal information? 5. Is data integrity checked to ensure copies of EHR are synchronized automatically?
Data aggregation	× Data set aggregated before records de-identified × Data set exchanged electronically without encryption × Data set exchanged manually without encryption × No assessment of potential for patient identification from non-identifying data elements × Assumption of implied consent to secondary use of data via consent to treatment.	≈ Basic access control in use (eg. password only with good password hygiene) ≈ Patients informed that some of their data may be used for secondary purposes but only a general consent sought.	✓ Strong access controls in use ✓ Encryption is used ✓ Patients informed of secondary data use ✓ Patient consent sought for specific uses ✓ Internet & network security protocols in use ✓ Data integrity checking is used ✓ Virtual Private Network in use ✓ Record collection limited to essential data elements ✓ System audits and access monitoring active	1. Is data de-identified before being aggregated for secondary use unless identification is a requirement by law? 2. Are patients made aware of potential secondary uses of their data? 3. Are patients given the opportunity to deny consent to secondary use of their data even if it is to be de-identified? 4. Has the potential to re-identify de-identified data been investigated and reduced or eliminated? 5. Is the aggregated data set encrypted? 6. Is the use of the data set limited to its intended purpose?

Figure 4. *Example Risk Management Tool for EHR Privacy*

Discussion and Implications:

As a nationally aggregated dataset, the NHMD is a high value information asset especially for research and funding organizations. AIHW has demonstrated in a trial that the data included in the NHMD can be used for data matching of individual patient records across the morbidity database and the residential aged care database (AIHW 2003). These two databases contain data on some of the same patients but the data is collected in very different circumstances by different personnel and for different reasons. Data matching records across unrelated databases is commonly referred to as record linkage. In the AIHW trial, the collecting organizations would not have been aware at the time their data was collected that the NHMD would be used for further, tertiary, record aggregation. It would have been virtually impossible for the collecting organization to answer 'yes' to questions 3, 4, or 6 in the Data Aggregation row in Figure 4. In this respect, record linkage activities demonstrate a lack of transparency, a failure to seek consent, and a failure to limit the use of collected data. Linked record sets are intended for research purposes and not for primary health care delivery. But the resulting linked record set contains even more detail about individuals, which may enable re-identification. It is also almost certain to include incorrectly matched records. Unauthorised access or disclosure of these linked records pose a moderate to high level of risk to patient privacy, Figure 3.

Personal EHR (PEHR) are thought to offer a way of giving the individual greater control over their personal information and therefore greater privacy. Not surprisingly though, PEHR are also subject to privacy and security risks. For example, removable storage devices are easily lost or damaged. In the context of morbidity data reporting, the data must always be accessible by the hospital. With multiple copies of the EHR in use, it is almost certain that over time the content of the PEHR will differ significantly from the versions stored at the health care facilities visited by the patient. Thus patient held records appear to be of little benefit with respect to morbidity data reporting. In fact, PEHR, in the context of NHMD, are likely to lead to additional risks requiring additional management controls and additional cost.

To be effective, risk assessments need to be performed on a regular basis so that timely decisions can be made about appropriate treatments. This paper has demonstrated how privacy risk assessment can be reduced to a simple set of questions for each risk factor using qualitative methods. The PRMT above is an example based on four key risk factors. It should not be treated as a comprehensive assessment tool. It may be used as a quick guide to EHR risks and as a checklist to focus further, more detailed risk assessments to suit specific risk contexts.

References:

AIHW. 2003. Feasibility study on linking hospital morbidity and residential aged care data to examine the interface between the two sectors. Australia
APF. 2006. Health E Link NSW. Australian Privacy Foundation Inc.
AusCert, and ALEA. 2006. Australian Computer Crime and Security Survey. AusCert and Australian Law Enforcement Agencies.
AIHW. 2006. National Hospital Morbidity Database (AIHW). AIHW National hospital morbidity database (NHMD).
Cth. Privacy Act 1988.
SAI. 2006. HB 167:2006 Security Risk Management. Sydney: Standards Australia.
SAI. 2003. HB 174-2003 Information security management - Implementation guide for the health sector. Sydney: Standards Australia International.
SAI. 2004. HB 231:2004 Information Security Risk Management Guidelines. Sydney: Standards Australia.
Stanton, Jeffrey M., Kathryn R. Stam, Paul Mastrangelo, and Jeffrey Jolton. 2005. Analysis of end user security behaviors. Computers & Security 24, no. 2:124-133.
WHS Qld. 2007. Slips, trips, and falls prevention. Brisbane: Queensland Government.

Acknowledgements:

I would like to thank Evelyn Hovenga for her leadership, inspiration, and support.

Contact Details:

e-mail: m.madsen@cqu.edu.au