EHR Privacy Risk Assessment Using Qualitative Methods

Maria Madsen
CQUniversity, Gladstone, Queensland
EHR Privacy Risk Assessment
A Systems Perspective

Compliance Need

• Perform privacy risk assessments on existing, upgraded, and new health information systems.

Problems

• Few people have security or system expertise needed
• Laws and standards provide general guidance but not detailed methods
• Full PRA consumes time and other resources
Privacy Risk Assessment
A Systems Perspective

Possible Solution
- Make privacy risk assessment easier & more consistent using a checklist approach – a method commonly used for WHS risk assessments
- Provide a Risk Management Tool (e.g. WHS Qld. Slips, Trips, and Falls)

Possible Methods
- Qualitative Risk Assessment Approach
- Use existing information from expert sources (Cth Law, AusCert, APF, SAI)
- Focus on uses & users (Activity Theory)
Privacy Risk Assessment
The Risk Management Approach

5 Step Cycle
- Establish the Context
- Identify the Risks
- Analyse the Risks
- Evaluate the Risks
- Treat the Risks

Repeat as Necessary

Tabulate Analysis Results

Transform Table into Risk Management Tool with simple Yes/No questions
Establish the Context

Focus on activities of EHR uses & users

Example Data Asset

The National Hospital Morbidity Dataset (NHMD)

2 Cases Considered:

1. Mandatory Reporting – Aggregated Data has no data elements that directly identify individuals. (secondary use)


Hospital Information Systems

Step 1

Security Management System
- Technical & Human components

Information Privacy depends on Information Security

Two Types of Use
- Authorised
- Unauthorised

End User Security Behaviours (Stanton et. al 2005)
- Unintentional (In)security
  - most common/likely
  - (e.g. leaving computer logged in when away from desk)
**Identify the Risks**

**Four Risk Factors Considered**
1. External Access (Internet)
2. Internal Access (Network)
3. Record Linkage (Unrelated Data Sets)
4. Patient-held Records (Portable Media)

**Threats**
*(what can go wrong)*
- Authorised access/Unauthorised use
- Unauthorised access
- Unexpected/Unintended use of collected data
- Re-identification from fields in linked records
- Data Errors

**Risks**
- Unauthorised disclosure
- Discrimination based on disclosed information
- Identity Theft
- Formal privacy breach complaint
- Incorrect Information disclosed

Step 3

Analyse the Risks

Threats From Secondary & Tertiary Uses

- ALMOST CERTAIN
  - Errors - incorrect, inaccurate data
- LIKELY
  - Patient identified from combination of non-identifying data elements
- POSSIBLE
  - Patient identified from more detailed data in linked datasets.
- UNLIKELY
  - Patient not informed. Express Consent not given.

Consequences For Hospitals & Patients

- CRITICAL
  - Embarrassment
  - Inconvenience
  - Frustration
- MAJOR
  - Loss of income
  - Legal penalty
  - Identity theft
- MODERATE
  - Some loss of consumer confidence
- MINOR
  - Discrimination
  - Identity theft
  - Lost consumer confidence

Qualitative analysis requires judgement of likelihood and consequences.
Evaluate the Risks

A Risk Assessment Matrix is provided in HB: 174-2003, p. 25
<table>
<thead>
<tr>
<th>Treatment Type</th>
<th>Technology Treatments (Barrier Controls)</th>
<th>Policy Treatments (Behavioural Controls)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk avoidance</td>
<td>Disconnect from network and/or internet</td>
<td>Decommissioning equipment procedure</td>
</tr>
<tr>
<td>Likelihood Reduction (Most Common)</td>
<td>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</td>
<td>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</td>
</tr>
<tr>
<td>Consequence reduction</td>
<td>intrusion detection systems, file integrity assessment tools</td>
<td>system audit policy, monitoring system access and use procedures,</td>
</tr>
<tr>
<td>Risk transference</td>
<td>Not applicable</td>
<td>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 system]</td>
</tr>
<tr>
<td>Risk retention</td>
<td>Too costly or not available</td>
<td>business continuity management, incident management procedures, forensic plan</td>
</tr>
</tbody>
</table>

(Sources: AusCert et. al 2006, SAI HB 231:2004, pp.17-31)
Privacy Risk Assessment
Putting it all together…

<table>
<thead>
<tr>
<th>Risk Factors</th>
<th>Threat (Example)</th>
<th>Risks</th>
<th>Likelihood</th>
<th>Consequences (Loss of consumer confidence)</th>
<th>Risk Level</th>
<th>Likelihood Reduction Treatment/Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>External Access via Internet</td>
<td>Poor online security at user’s end</td>
<td>Unauthorised Use/Disclosure</td>
<td>Possible</td>
<td>Moderate</td>
<td>Moderate/Low</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>Internal Access</td>
<td>Poor security hygiene (passwords shared)</td>
<td>Unauthorised Use/Disclosure</td>
<td>Almost Certain</td>
<td>Moderate</td>
<td>Moderate</td>
<td>User Training</td>
</tr>
<tr>
<td>Patient Held Record</td>
<td>Loss of storage media and records</td>
<td>Unauthorised Use/Disclosure</td>
<td>Likely</td>
<td>High</td>
<td>Moderate</td>
<td>Patient Education</td>
</tr>
<tr>
<td>Record Linkage</td>
<td>Re-identification from more detailed data</td>
<td>Unauthorised Use/Disclosure</td>
<td>Possible</td>
<td>High</td>
<td>Moderate</td>
<td>Security Behaviour Training for Record Users</td>
</tr>
</tbody>
</table>

A consequence may have different risk level depending on context.
### An EHR Privacy Risk Management Tool:
Supports Evaluation of Privacy Risks in EHR System

<table>
<thead>
<tr>
<th>Risk Factor</th>
<th>High Risk</th>
<th>Moderate Risk</th>
<th>Low Risk</th>
<th>Example Risk Assessment Questions (Yes/No)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Very Likely to Cause Privacy Breach</td>
<td>Some risk of breach &amp; Short term controls</td>
<td>Less likely to result in privacy breach &amp; possible controls</td>
<td>1. Are data transmissions encrypted?</td>
</tr>
<tr>
<td>External access to EHR system</td>
<td>× Minimal or missing access controls (e.g. password only identity verification with poor password hygiene)</td>
<td>≈ Basic access control in use (e.g. password only with good password hygiene)</td>
<td>✓ Strong access controls in use</td>
<td>2. Are users educated about the risks involved in accessing EHR using the internet?</td>
</tr>
<tr>
<td></td>
<td>× Inadequate network and/or internet security</td>
<td>≈ Basic network and internet security protocols used</td>
<td>✓ Encryption is used</td>
<td>3. Are users trained to use the system?</td>
</tr>
<tr>
<td></td>
<td>× Insufficient security training and education of users including personnel and patients</td>
<td>≈ Infrequent monitoring of system access</td>
<td>✓ Users are informed and trained.</td>
<td>4. Is the system robust against user error?</td>
</tr>
<tr>
<td></td>
<td>× Encryption is not used for email</td>
<td></td>
<td>✓ Internet &amp; network security protocols in use</td>
<td>5. Are people given the option to opt out of using the system?</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>✓ Data integrity checking is used</td>
<td>6. Is connection secure end to end?</td>
</tr>
</tbody>
</table>

**From Risk Analysis**

**Based on Controls**
Discussion and Implications:
Applying the RMT to NHMD and Personal EHR held by patient

- Privacy Risk when NHMD is used as intended
  - set of de-identified patient records containing limited data elements
  - used for secondary purposes
    - Mandatory reporting
    - Research
- Poses low to moderate risk to individual privacy

- Privacy Risk when NHMD is linked with other data sets (i.e. Aged Care)
  - Consolidated records increase value of data asset
  - Data Errors introduced through matching method, incorrect records created
  - Re-identifying individuals more likely
- Increased risk to patient privacy (mod-high)

- Privacy Risk when data required for NHMD is kept by patient
  - Synchronization of data copies required
  - Patient training/education required
  - Additional security technology required
  - Increased likelihood of loss or damage
- Multiple copies of data - high risk to patient privacy
- Patient controlled copies – mod-high risk to patient privacy
Conclusion

PROBLEM
• Assess EHR Privacy Risks given limited resources

QUAL. METHOD
• Relatively simple and reliable (though subjective)
• Useful for PRA – difficult to measure human factors using quantitative methods

PRIVACY R.M. TOOL
• Requires refinement before application and use
• Specific risks need to be considered in context
• Re-useability of checklist could save time & money

Many Thanks to …
Prof. Evelyn Hovenga for her support &
All of you for your kind attention