BE WHAT YOU WANT TO BE

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)

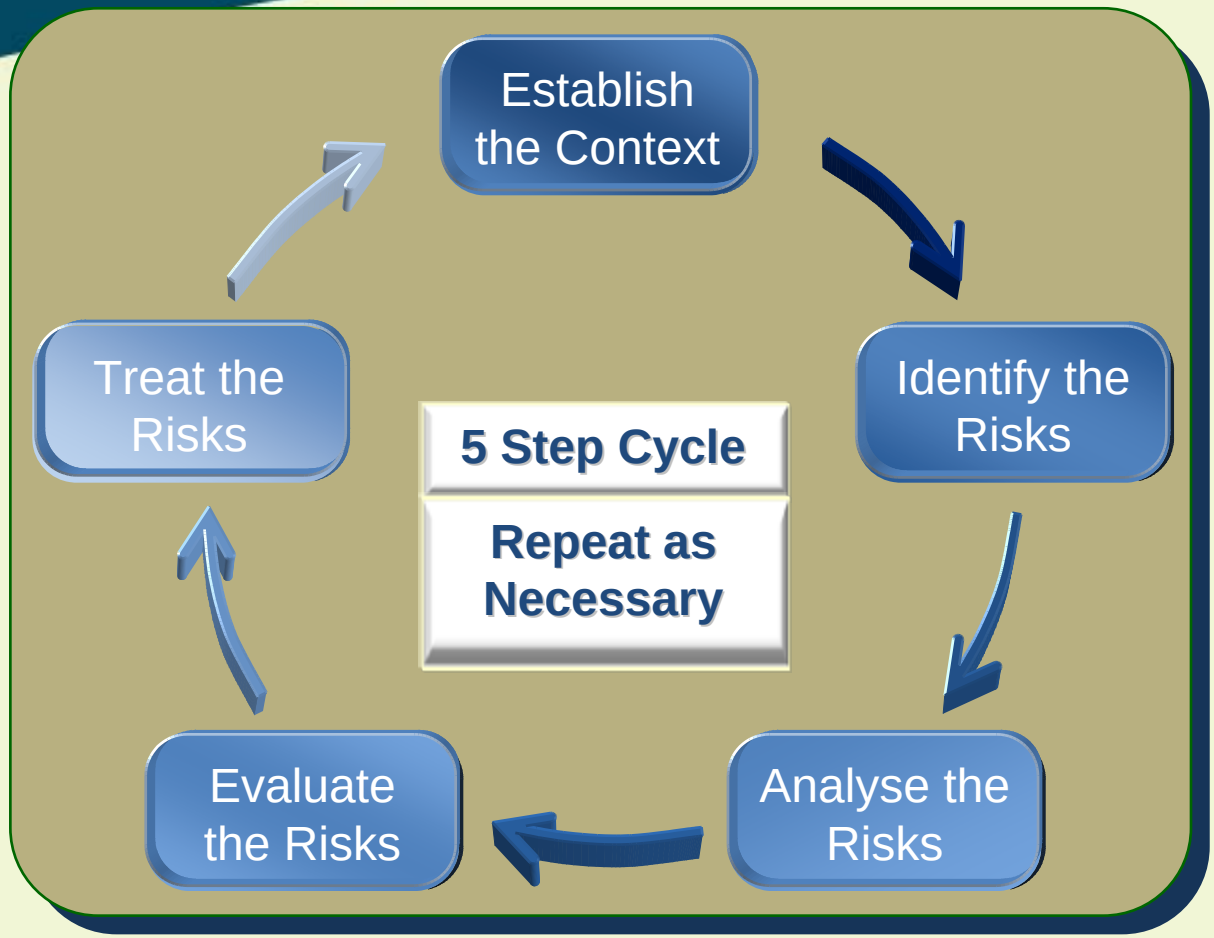
Possible Methods

- 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

Process



Tabulate Analysis Results

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

Establish the Context

Hospital Information Systems

Step 1

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**)
2. **Record Linkage Study** – record matching across health services trialled by Australian Institute of Health and Welfare (AIHW 2003) (**tertiary use**)

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

Step 2

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

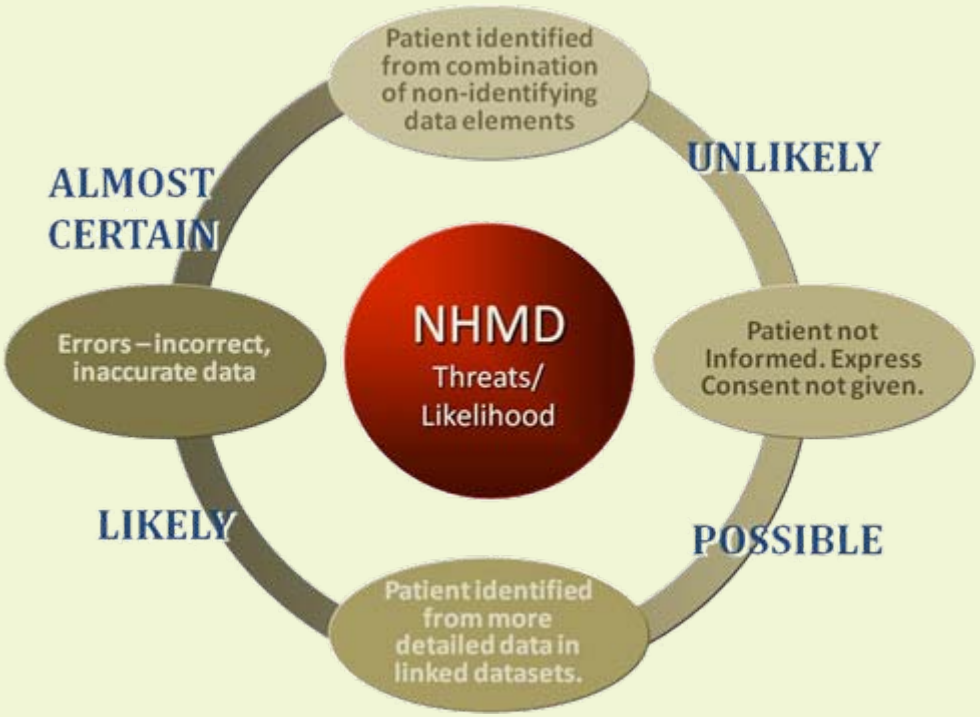
- Unauthorised disclosure
- Discrimination based on disclosed information
- Identity Theft
- Formal privacy breach complaint
- Incorrect Information disclosed

(Sources: APF 2006, Aust. Privacy Act 1988, SAI – HB 167:2006; HB 174-2003; HB 231:2004)

Analyse the Risks

Step 3

Threats From Secondary & Tertiary Uses



Consequences For Hospitals & Patients

Qualitative analysis requires judgement of likelihood and consequences.

Evaluate the Risks

Step 4

A Risk Assessment Matrix is provided in HB: 174-2003, p. 25

Treat the Risks

Step 5

Treatment Type	Technology Treatments (Barrier Controls)	Policy Treatments (Behavioural Controls)
Risk avoidance	Disconnect from network and/or internet	Decommissioning equipment procedure
Likelihood Reduction (*Most Common*)	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 system]
Risk retention	Too costly or not available	business continuity management, incident management procedures, forensic plan

(Sources: AusCert et. al 2006, SAI HB 231:2004, pp.17-31)

Privacy Risk Assessment

Putting it all together…

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

A consequence may have different risk level depending on context.

An EHR Privacy Risk Management Tool:

Supports Evaluation of Privacy Risks in EHR System

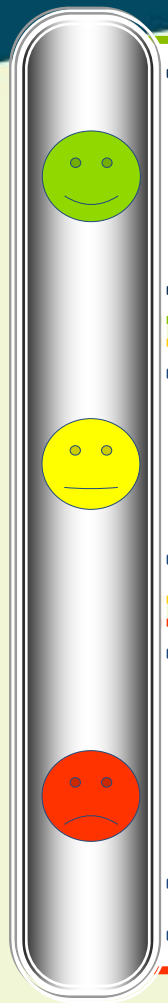
PRMT

Risk Factor	High Risk Very Likely to Cause Privacy Breach	Moderate Risk Some risk of breach & Short term controls	Low Risk Less likely to result in privacy breach & possible controls	Example 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?

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

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

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