Interpreting International Governance Standards for Health IT use within General Medical Practice

HIC 2014
RACHEL J MAHNCKE & PATRICIA A H WILLIAMS
EHEALTH RESEARCH GROUP, SCHOOL OF COMPUTER AND SECURITY SCIENCE
EDITH COWAN UNIVERSITY, PERTH, AUSTRALIA
Is security like swimming with sharks?

"I discovered I scream the same way whether I'm about to be devoured by a Great White or if a piece of seaweed touches my foot."
Axel Rose (Guns'n'Roses)

Or rather, how do we protect health data, avoid being caught unaware and avoid being severely bitten?
What is the problem?

- General practices in Australia recognise the importance of comprehensive protective security measures.
- With privacy law reform in March 2014, renewed focus within Australian healthcare on how to address such requirements.
- The governance component of information security is still insufficiently addressed in practice.
- Governance implies accountability, responsibility, monitoring and reporting to demonstrate legal and ethical compliance to information security practice, and to ensure that all computer and information security processes are documented and followed..... Or more simply
Information Governance is.....
Or.....

- Yes....working with standards CAN be exciting and rewarding !!!!
Royal Australian College of general Practitioners (RACGP) publish the Computer and Information Security Standards (CISS) for General Practice.

Thirteen standards (including privacy).

The CISS (2013) is designed to assist practices to meet their legal and professional obligations with respect to protecting their computer and information systems standard.
Protection =

[Image of Swiss cheese]

This standard demonstrates the relationship between governance and the management of information security.

Standard offers a framework against which to assess and implement the governance components of information security.

Provides strategic principles and processes, and forms the basis for establishing a positive information security culture.
“Seriously, information governance is no where near as hard as this....”
Methodology

- Based on the literature, analysis of the ISO/IEC 27014:2013 standard and feedback provided from five focus group interviews and three Participant Observations.

- The interpretation of ISO/IEC 27014: 2013 into a framework that can be applied directly and practically into healthcare is relevant given the emergence of information security governance in this sector.

- This analysis demonstrates that such a standard can be supported by and integrated within other frameworks, such as the RACGP CISS (2013).
Processes for each Principle are undefined in the standard;

Therefore to be implemented, the organisation would need to determine the missing Processes criteria in order to perform each Principle.

<table>
<thead>
<tr>
<th>Principles</th>
<th>Evaluate</th>
<th>Direct</th>
<th>Monitor</th>
<th>Communicate</th>
<th>Assure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Principle 1</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Principle 2</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Principle 3</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Principle 4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Principle 5</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Principle 6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

Table 1. Mapping the ISO27014:2013 processes to the principles.
For each of the *Perform* and *Enable* functions there are a set of associated requirements for the five Processes.

There are twenty three *Perform* and *Enable* tasks provided by the standard in total.

Within the general practice environment, the *Perform* tasks are likely to be conducted by the practice staff, and the *Enable* tasks by Executive Management.

The outcome of this analysis and resultant responsibility for tasks, is significantly different to that proposed in the standard.
A Model for General Practice

Figure 1 is adapted from the ISO/IEC 27014:2013 standard, it represents the relationship between the standard and CISS.
Interpretation of an information security governance model for general medical practice

- Adaptations to the ISO standard model are the addition of the Enable and Perform processes, the interrelationship between RACGP CISS (2013) ISM and governance, encapsulation of the information security governance domain, and the juxtaposition of the Governing Body and Executive Management.

- Associations between Processes, Governing Body, Executive Management, Perform and Enable as relates to information security.

- The model provided in the standard does not include representation of the interrelationship of the Principles to other components in the model.
Incorporating Governance Aspects from the CISS (2013) Standards

- Four of the twelve CISS (2013) standards relate to governance:
  - Standard 1: Roles and responsibilities;
  - Standard 2: Risk assessment;
  - Standard 3: Information security policies and procedures; and
  - Standard 5: Business continuity and information recovery.

- CISS Compliance Checklist that:
  - “is designed to help general practices assess, achieve and sustain compliance with the 12 Standards that comprise good practice in computer and information security”.

Thus, the proposed framework could provide general practice organisations with a standalone framework to measure information security governance capability whilst utilising standards such as the CISS (2013) operational framework, to provide the information security management measures.

Implementing information security governance principles alone without a measurement of capability does not provide assurance that governance processes are effective.
Questions which remain unanswered in the ISO27014:2013 standard

- Principle 5: Foster a security-positive environment is not embedded into the standards Executive Management Enable processes;
- There is no mention of Business Continuity, although implied within Risk appetite;
- The Assure Process is notably missing in a number of areas within the standard;
- Accountability is mentioned in one Process, and yet forms a large component of governance;
- The relationship between the Principles and Processes is undefined;
- Enable and perform are not defined in the standard;
- Processes which refer to the Governing body are repeated for both enable and perform, but the wording is not applicable to Executive Management. This creates uncertainty when reading and understanding the standard;
- Principles map into the Processes, but the Processes do not map to the Principles; and some Principles almost get no mention within the standards.
Conclusion

- An analysis of the standard was performed.
- It demonstrates an application of the standard at a strategic level to inform existing development of an information security governance framework.
- This work is unique as such interpretation for the Australian healthcare environment has not been undertaken before.
See, security governance is not as difficult as...

however...
...reading and getting help interpreting the standards will help!
Questions?

- Rachel J Mahncke & Patricia A H Williams
- eHealth Research Group, School of Computer and Security Science
- Edith Cowan University, Perth, Australia
- rmahncke@our.ecu.edu.au