12-4-2013

The Applicability of ISO/IEC27014:2013 For Use Within General Medical Practice

Rachel J. Mahncke
Edith Cowan University

DOI: 10.4225/75/5798124731b3f
2nd Australian eHealth Informatics and Security Conference, held on the 2nd-4th December, 2013 at Edith Cowan University, Perth, Western Australia

THE APPLICABILITY OF ISO/IEC27014:2013 FOR USE WITHIN GENERAL MEDICAL PRACTICE

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

Abstract

General practices are increasingly cognizant of their responsibilities in regards to information security, as is evidenced by professional bodies such as the Royal Australian College of General Practitioners (RACGP) who publish the Computer and Information Security Standards (CISS) for General Practices. Information security governance in general medical practice is an emerging area of importance. As such, the CISS (2013) standard incorporates elements of information security governance. The International Organization for Standardization (ISO) released a new global standard in May 2013 entitled, ISO/IEC 27014:2013 Information technology -- Security techniques -- Governance of information security. The release of this revised ISO standard, which is applicable to organisations of all sizes, offers a framework against which to assess and implement this governance component of information security within general medical practice. This paper reports on an analysis of this standard to determine how it could be applied to Australian general practice. The paper further reports on two qualitative interviews with information security experts relating to the suitability of utilising this standard within general practice. The results confirm that the governance component of information security. which is currently insufficiently addressed within general practice, requires support in the form of standards, however that developing a security culture is crucial to good governance in medical information security.

Keywords
ISO/IEC 27014:2013; Information Security Governance; General Medical Practice; Focus Group Interviews; RACGP CISS (2013)**.**

INTRODUCTION

General practices are the first point of contact for patients requiring health related care (RACGP, 2005). General practitioners refer patients onto specialists or hospitals for further expert medical treatment as required. Further, hospitals' will mostly discharge patients into the long-term care of their general practitioner. As such, general practices are involved in a high percentage of the information exchanges that occur to support the continuity of patient care (NEHTA, 2006).

The implementation of reliable information security practices within general practice is critical to the protection and secure exchange of confidential patient information. Since the technology to securely store and transmit electronic health information is well developed, the issue appears to be compliance in term of adhering to information security policies and procedures (Williams, 2013). Further, issues arise when the security protection enforced by one healthcare provider differs from that enforced by another to whom the information has been transferred (Sharpe, 2005; Williams & Mahncke, 2006). Protection of private health information therefore is both a technical and people orientated endeavour (ISO/IEC 27002, 2005; Williams, 2006a). These concerns bring medical data into the same sphere of risk as other networked data, however with added complexity and significance due to patient consent and legal protection requirements (Williams & Mahncke, 2006).

Confidential health information collected by general practices needs to be adequately protected if their information contributions are to meet expected legal, social and ethical requirements (Pharow & Blobel, 2004). Securing patient health information requires appropriate measures in regards to technologies, policies, and procedures as well as staff who are trained and aware of these security processes (Williams, 2006a). Whilst security policies are considered an important aspect of information security practice, Williams (2007) found that few practices had complete formal written security policies. Further, this research has confirmed that the same is applicable in 2013. Mapping information security processes within two general practices has determined that medical practices are not fully compliant with best practice information security industry standards, such as the RACGP Computer and Information Security Standards (CISS), 2013. General practices need to take responsibility for their information thereby avoiding the loss or theft of confidential patient information.

Information security governance in general medical practice is an emerging challenge (Mahncke & Williams, 2013). With the release of the RACGP CISS (2013) standards, aspects of information security governance, such as compliance and communicating security expectations, are evident. CISS (2013) has been mapped to the ISO/IEC 27014:2013 Information technology -- Security techniques -- Governance of information security standard to determine to what degree information security governance has already been embedded into CISS (2013). The outcome found that CISS (2013) remains predominantly an operational document based on the ISO/IEC27799:2008 Health informatics -- Information security management in health using ISO/IEC 27002. This paper provides an outline of the governance standard and an analysis if its applicable to general medical practice.

ISO/IEC 27014:2013

The ISO/IEC 27014:2013 was released on the 15th of May 2013. Governance of information security is a "system by which an organisation's information security activities are directed and controlled" (ISO/IEC 27014:2013). ISO/IEC 27014:2013 is part of the ISO/IEC 27000 series of standards. This new standard was released as both an ISO/IEC 27014 and ITU-T recommendation X.1054 (IRCA, 2013). "Proper governance of information security ensures alignment of information security with business strategies and objectives, value delivery and accountability. It supports the achievement of visibility, agility, efficiency, effectiveness and compliance" (ISO27001security, 2013).

This standard is "specifically aimed at helping organizations govern their information security arrangements" (ISO27001security, 2013). The standard provides "guidance on concepts and principles for the governance of information security, by which organisations can evaluate, direct, monitor, communicate and assure the information security related activities within the organisation" and is "applicable to all types and sizes of organisations" (ISO/IEC 27014:2013).

The relatively brief, eleven page standard outlines the governance of information security concepts and provides a framework of six principles and five frameworks (ISO/IEC 27014:2013). The standard views the governance of IT as overlapping with the governance of information security, both these elements being constituent parts of the broader concept of organisational governance (ISO/IEC 27014:2013) as shown in Figure 1.

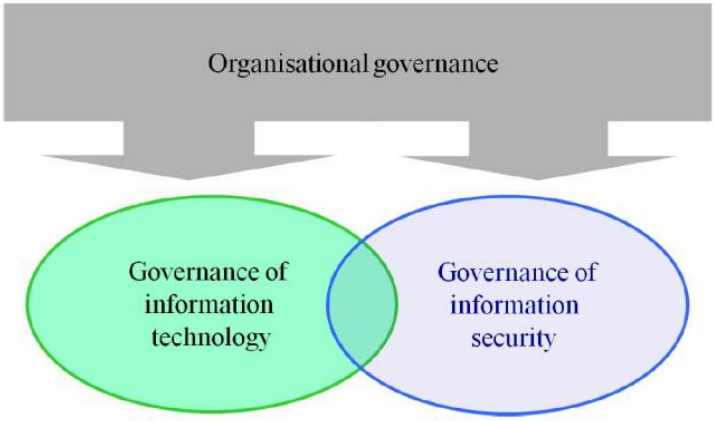

Figure 1: Relationship between governance of information security and governance of information technology (ISO/IEC 27014:2013)

"Governance of information security should ensure that information security activities are comprehensive and integrated" (ISO/IEC 27014:2013). The standard specifies six high-level "action-oriented" information security governance principles (ISO/IEC 27014:2013) such as:

- **Principle 1** - Establish organisation-wide information security
- **Principle 2** - Adopt a risk-based approach
- **Principle 3** - Set the direction of investment decisions
- **Principle 4** - Ensure conformance with internal and external requirements
- **Principle 5** - Foster a security-positive environment

- **Principle 6** - Review performance in relation to business outcomes

The five governance processes ("evaluate", "direct", "monitor", "communicate" and "assure") are distinct tasks which are implemented by the governing body and executive management (Figure 2).

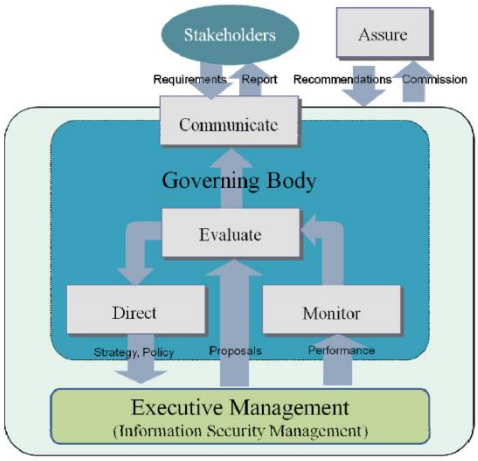

Figure 2: Implementation of the governance model for information security (ISO/IEC 27014:2013)

These distinct tasks are outlined from the standard in Table 1.

Processes	Definition (ISO/IEC 27014:2013)
Evaluate	Considers the current and forecast achievement of security objectives based on current processes and planned changes and determines where any adjustments are required to optimise the achievement of strategic objectives in future.
Direct	By which the governing body gives direction about the information security objectives and strategy that need to be implemented. Direction can include changes in resourcing levels, allocation of resources, prioritisation of activities, and approvals of policies, material risk acceptance and risk management plans.
Monitor	"Monitor" is the governance process that enables the governing body to assess the achievement of strategic objectives.
Communicate	"Communicate" is the bi-directional governance process by which the governing body and stakeholders exchange information about information security, appropriate to their specific needs. One of the methods to "communicate" is information security status which explains information security activities and issues to stakeholders, examples of which are shown in Annexes A and B.
Assure	By which the governing body commissions independent and objective audits, reviews or certifications. These will identify and validate the objectives and actions related to carrying out governance activities and conducting operations in order to attain the desired level of information security.

Table 1: Definition of Processes (ISO/IEC 27014:2013)

These tasks and processes were analysed to determine how it could be applied to Australian general practice.

METHOD

The mapping and analysis of ISO/IEC 27014:2013 is one element of a doctoral research project to develop an Information Security Governance Framework (ISGF), and to apply and test the resultant framework within the general practice environment. As such a flexible qualitative research approach was adopted. This paper reports on the initial outcomes. The method chosen was Action Research, as it would enable iterative changes to the framework to be made throughout the research process. All forms of qualitative research are known for their ability to learn about and understand the "perspectives of others rather than imposing the researcher's own views, biases, and theories in explaining differences across populations or communities in beliefs and behaviours" (Schensul, 2009).

An action research approach was considered the most appropriate for this research as active participation would be required as part of the 'information system' (inclusive of people as a social constituent of the information system) under investigation. Studies suggest that the action research approach is particularly suited to

information security and general practice research (Williams 2006b; Hampshire, Blair, Crown, Avery & Williams, 1999). In action research, the action researcher is concerned about creating change whist simultaneously studying the process (Myers, 2009). Through collaboration both the researcher and the subjects learn from the context being studied (Myers, 2009). In its traditional form, action research involves cycles of "investigation, action planning, piloting of new practices, and evaluation of outcomes" (Cullen, 1998; Baskerville & Wood-Harper, 1996; McIntyre, 2008). At each stage of the collection and analysis of data, knowledge is generation (Somekh, 2008; Baskerville & Wood-Harper, 1996). The outcomes of action research are both practical and theoretical (Somekh, 2008; McIntyre, 2008). They are practical in the sense that the outcomes will inform security practice, and theoretical in that the knowledge generated will continue to have a lasting impact on changing practice through the publication of the research (Somekh, 2008). In research practice improvements in the action plan are incorporated into the next cycle by reflecting on participant feedback together with the experience of the previous cycle (Hampshire, Blair, Crown, Avery & Williams, 1999).

Research Design

The research comprises of two stages.

First Stage - Development and Validation of the Framework

Focus group interviews provide a means of validating the proposed governance framework. These interviews provide an opportunity to focus discussions and to examine, resolve, or come to a conclusion in relation to a particular problem under investigation (Krueger & Casey, 2009). The focus group method is a valid and tested qualitative research method.

During the focus group interviews, participants were asked to evaluate the applicable version of the framework, and asked the same set of ten semi-structured questions. Six participants, plus the researcher, were considered to be an ideal number of participants for each focus group interview. Following ethics approval and participant consent, focus group interviews were recorded with two electronic devices, an iPhone and Audacity software recorded on a laptop. The focus groups were each one hour in length.

Second Stage – Iterative Cycles of Participant Observations

Whilst the first stage of the research is reported on in this paper, a brief outline of the subsequent participant observation method that will be used in stage two is provided for clarification. The purpose of the second research cycle is to apply the framework within Australian general practice. During the participant observations, general practices will be asked to: map the governance framework to their actual practice, participate in a semi-structured interview and provide copies of their de-identified information security polices for triangulation analysis. The triangulation method will be further applied utilising the framework outcomes, interview answers and documented policies.

Content Analysis

The ISO/IEC 27014:2013 standard and the two interviews in question were transcribed from audio into Microsoft Word. The Microsoft Word document was analysed and coded by hand by the researcher and then imported into NVivo for a second qualitative analysis review. QSR's NVivo is qualitative analysis software, which utilises the traditional method of colour coding groups and themes, and rearranging the information into organised categories for analysis.

Analysis generally begins by conducting comparisons and contrasts within the data to extract themes and patterns (Schensul, 2009). The data analysis involved the detailed coding of the interview data. Coding categories vary according to the data under analysis. Dominant themes in the data were identified and examined. This was followed by revising, refining and testing the data against those detailed themes. Logical codes emerge as continuous evaluation and comparisons continue, producing a final set of codes that can be applied to the entire data set (Schensul, 2009). Further, a set of comments, memos, and analytic summaries can be utilised for overall analysis and interpretation (Schensul, 2009). The information security governance framework that is pivotal to this research was modified based on major themes identified in the analysis.

RESULTS

This section reports on the analysis of the ISO/IEC 27014:2013 standard and two interviews as part of the First Stage of the research.

Analysis of the ISO/IEC27014:2013 Standard

The ISO/IEC 27014:2013 standard was purchased and the electronic document imported into the NVivo software and analysed. The following themes were identified as shown in Table 2.

Major Themes identified in the ISO/IEC27014:2013 Standard	***Total # of occurrences***
First edition 2013-05-15	1
Stakeholder	3
Risk management approach	19
Processes	57
Principles	44
Organisational governance	3
Objectives of governance of information security	4
Information Security	8
Governing body	37
Governance of information security should include	12
Executive management	12
Desired outcomes from effectively implementing governance of information security	4
Compliance	4
Collaboration with WTSA UN agency	1
Applicable to all types and sizes of organisations	2
Align business objectives and strategies	2
Total	**213**

Table 2: NVivo analysis of the ISO/IEC27014:2013 Standard

Most notable outcomes from the coding and analysis of the standard:

- ISO/IEC 27014:2013 is a recommendation and is not enforceable (it is a normative reference);
- ISO/IEC 27014:2013 is applicable to organisations of all sizes;
- ISO/IEC 2714:2013 Provides guidance on:
    - Mandate essential for driving information security initiatives throughout the organisation;
    - Link between Management and Information Security Management Systems (ISMS);
    - Effective governance of information security – Reporting - Timely decisions; and
    - About information security-related activities.
- Desired Outcomes of ISO/IEC 2714:2013 for effectively implementing governance of information security include:
    - governing body visibility on the information security status;
    - efficient and effective investments on information security;
    - compliance with external requirements (legal, regulatory or contractual); and
    - an agile approach to decision-making about information risks.

Analysis of Interview 1

The Interview 1 participant is a healthcare security expert who has industry knowledge of the ISO/IEC 27014: 2013 standard under discussion. The participant has practical experience in the application of the standard. The participant was generous with their time and applying their knowledge to general medical practice environment. The major themes identified from the interview are shown in Table 3.

Topics discussed – Overall	**Total #**
Threat environment	12
Security training	2
People	2
Laws	7
IT Governance	7
ISO/IEC 27014:2013	26
ISGF (Mahncke)	39
FBI	5
CMMI	11
CISS (2011)	3
Checklist approach	2
Assurance to patients	6
Total	**122**

Topics discussed – specifically ISO/IEC 27014:2013	**Total #**
Worked on ISO27014 Committee that reviewed the standard	1
Useful	1
Roles and Responsibilities	1
Purpose of the 27014 standard	2
Need for ISO/IEC 27014: 2013	3
Lacks 'how to' details	5
Familiarity with ISO/IEC 27014: 2013	1
Applicable to organisations of all sizes	12
Total	**26**

Table 3: Outcomes of Interview 1

Analysis of Interview 2

The Interview 2 participant is a Chief Information Officer (CIO) for a large global organisation. The security expert had not viewed the ISO/IEC 27014:2013 standard prior to the interview. The major themes identified from the interview are shown in Table 4.

Topics discussed - Overall	**#**
27100 compliant	15
Security	26
Policies	3
ISO/IEC 27014: 2013	42
ISGF Mahncke	46
Future security plans	23
CMM	7
CISS	0
Total	**162**
Themes for ISO/IEC 2714:2013	**#**
Not see prior to interview 27014	1
Used by small businesses -Type of business Risk -Need to meet security requirements -General practices Sensitive information	6
Best practice -May never want to be ISO standardised, because of resources	1
Optimal practise -Makes sense for us to do that -Happy to move towards actually being accredited against that standard	5

-Can prove that we're optimally there	
Governance -Resources, most notably staff -Compliance -At the stage to do it now Restructure IT	9
Standard is good -Not prescriptive -It's very simple -It's not a big standard -Good to articulate the key principles It's a checklist Articulates the things you should try to achieve	9
-Principles Up to you Few principles Different interpretations	3
Continuous improvement	3
Review governance structure	2
Five processes	1
Disaster recovery appears to be missing from ISO/IEC 27014: 2013	2
Total	**42**

Table 4: Outcomes of Interview 2

DISCUSSION

The ISO/IEC 27014:2013 standard provides is a framework of five processes (evaluate, direct, monitor, communicate, and assure) and each process has associated 'perform' and 'enable' tasks. The processes show "a relationship between governance and the management of information security" (ISO/IEC 27014:2013). The tasks (Table 5) enable "the governance of information security and their interrelationships" (ISO/IEC 27014:2013).

Processes	**Perform (Done by the Governing Body)** *(ISO/IEC 27014:2013)*	**Enable (Done by Executive Management)** *(ISO/IEC 27014:2013)*
Evaluate	- respond to information security performance results, prioritize and initiate required actions. ensure that business initiatives take into account information security issue	submit new information security projects with significant impact to governing body ensure that information security adequately supports and sustains the business objectives
Direct	determine the organisation's risk appetite approve the information security strategy and policy allocate adequate investment and resource	promote a positive information security culture develop and implement information security strategy and policy align information security objectives with business objectives
Monitor	ensure conformance with internal and external requirements consider the changing business, legal and regulatory environment and their potential impact on information risk assess the effectiveness of information security management activities	select appropriate performance metrics from a business perspective provide feedback on information security performance results to the governing body including performance of action previously identified by governing body and their impacts on the organisation alert the governing body of new developments affecting information risks and information security
Communicate	report to external stakeholders that the organisation practices a level of information security commensurate with the nature of its business recognize regulatory obligations, stakeholders expectations, and business needs with regard to information security notify executive management of the results of any external reviews that have identified information security issues, and request corrective actions	instruct relevant stakeholders on detailed actions to be taken in support of the governing body's directives and decisions advise the governing body of any matters that require its attention and, possibly, decision
Assure	commission independent and objective opinions of how it is complying with its accountability for the desired level of information security	support the audit, reviews or certifications commissioned by governing body

Table 5: Perform and enable framework for the ISO/IEC 27014:2013 processes

It is unclear how the Principles 1-6 specified in ISO/IEC 27014:2013 map into this process framework, as this is not demonstrated in the Standard. Mapping the Principles to the tasks listed in Table 5 above demonstrates that aspects of the principles are evident in the tasks. For example, Principle 1 maps into all of the processes but Principle 6 maps only to Communicate and Assure processes. The Principles in the standard are brief, they describe what should happen but does not prescribe when, how or by whom the principles would be implemented. The reason provided in the standard are that "these aspects are dependent on the nature of the organisation implementing the principles" (ISO/IEC 27014:2013).

Thus, with this in mind, the major themes were identified during the analysis of the standard and the two interviews, and are addressed as follows.

Governing Body

The Governing Body is "person or group of people who are accountable for the performance and conformance of the organisation" (ISO/IEC 27014:2013). The Governing Body is an important aspect of the standard. According to (ISO/IEC 27014:2013), the role of the Governing Body is critical to implementation success, and arguably the most valued contribution this standard provides. The Governing Body is appointed by Executive Management. However, Executive Management is a "person or group of people who have delegated

responsibility from the governing body for implementation of strategies and policies to accomplish the purpose of the organisation" (ISO/IEC 27014:2013).

Analysis of the ISO/IEC 27014:2013 (Table 6) determined that the responsibilities of the Governing Body relate to:

Governance responsibilities, such as accountability	Require that the six principles be applied
To address conformance and compliance issues	Key focus is to ensure the organisation's approach to information security
Allocate resources	Appoint people with security responsibilities
Perform processes	should require, promote and support coordination of stakeholder activities to achieve a coherent direction for information security
Authority to implement six principles	should ensure that information security is integrated with existing organisation processes

Table 6: Governing Body responsibilities

"Governance of information security provides a powerful link between an organisation's governing body, executive management and those responsible for implementing and operating an information security management system" (ISO/IEC 27014:2013).

Risk

Risk, and its inclusion in an information security governance framework, has been discussed in the first three interviews and these outcomes and published by Mahncke and Williams (2013). Further, the two interview participants raised the issue of including a risk management approach into an information security governance framework.

Interview 1

The participant from Interview 1 felt that the ISO/IEC 27014:2013 standard was:

- Useful; a complimentary document to the other ISO standards;
- There was possibly no need for the ISO/IEC 27014:2013 standard;
- The standard lacks implementation detail and meaning;
- The standard could be applicable to organisations of all sizes, possibly more so in a larger medical centre and large organisations; and
- That there would be associated costs (for people) to implement the standard.

Interview 2

The participant from Interview 2 stated that the ISO/IEC 27014:2013 standard was

- Optimal practise;
- That it makes sense to do but that organisations may never want to be ISO standardised, because of the required resources;
- Happy to move towards actually being accredited against that standard;
- Should be used by general practitioners because of their sensitive information;
- Necessary for compliance;
- The standard is good as it is not prescriptive, simple, good to articulate the key principles;

- Few principles means it is useful to the organisation; but there could be different interpretations;
- The standard encompasses continuous improvement; and
- Reviews the governance structure but that disaster recovery appears to be missing from the standard.

Final thoughts

Arguably, the standard raises more questions than answers, such as: How do the principles and processes work together; how are organisations to implement the standard; what are the added benefits of implementing the standard and why is the 'Assure' process missing in a number of references to processes. An important contribution of the ISO/IEC 27014:2013 standard is its endeavour to "establish a positive information security culture, the governing body should require, promote and support coordination of stakeholder activities to achieve a coherent direction for information security. This will support the delivery of security education, training and awareness programs." (ISO/IEC 27014:2013).

A search of the scholarly literature determined that there are very few published reviews of the standard to date. One article has been published to date which refers to the ISO/IEC 27014:2013 standard. The article by Williams, Hardy and Holgate (2013) entitled *Information security governance practices in critical infrastructure organizations: A socio-technical and institutional logic perspective*, however this has limited applicability in the healthcare environment. ISO/IEC 27014:2013 is a new standard which has not been implemented in the general medical practice environment to date. This research aims to interpret and implement new standard.

CONCLUSION

In an environment that is embracing e-health, the importance of information security governance is emerging as a key factor in the assurance and protection of healthcare information. To complement and build on developments in information security practices, investigation into effective governance processes that can be aligned with, and fed into by, information security practice has been undertaken. The release of the new ISO/IEC 27014: 2013 standard which is applicable to organisations of all sizes, offers a framework against which to assess and implement this governance component of information security within general medical practice. This standard was analysed to determine how it could be applied to Australian general practice.

ISO/IEC 27014:2013 , as a new standard, has not been implemented in the general medical practice environment to date. The standard specifies six high-level "action-oriented" information security governance principles and provides a framework of five processes (evaluate, direct, monitor, communicate, and assure) which each have associated 'perform' and 'enable' tasks. The processes show "a relationship between governance and the management of information security" (ISO/IEC 27014:2013). An important contribution of the ISO/IEC 27014:2013 standard is its endeavour to "establish a positive information security culture".

The standard acknowledges the role of the human element in security by supporting the delivery of security education, training and awareness programs through the Governing Body. The Governing Body is "person or group of people who are accountable for the performance and conformance of the organisation" (ISO/IEC 27014:2013). The Governing Body is an important aspect of the standard. According to (ISO/IEC 27014:2013), the role of the Governing Body is critical to implementation success, and arguably the most valued contribution this standard provides.

REFERENCES

Baskerville, R., & Wood-Harper, A.T. (1996). A critical perspective on action research as a method for information systems research, *Journal of Information Technology, 11*(3):235-246.

Cullen, J. (1998). The needle and the damage done: Research, action research , and the organizational and social construction of health in the "information society", *Human Relations. 51*(12): 1543-1564.

Hampshire, A., Blair, M., Crown, N., Avery, A., & Williams, I. (1999). Action research: a useful method of promoting change in primary care? *Family Practice; 16*(3): 305.

IRCA. 2013). *ISO/IEC 27000: get to know the family*. Retrieved September 30, 2013 from http://www.irca.org/en-gb/resources/INform/archive/issue25/Features/ISO-IEC-27000/

ISO27001Security. (2013). *ISO/IEC 27014. 2013*. Available from http://www.iso27001security.com/html/27014.html

International Standards organisation. (2005). *ISO/IEC 27002-2005 International standard - Information technology - Security techniques - Code of practice for information security management*. Available from http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103 uis.georgetown.edu/departments/eets/dw/GLOSSARY0816.html

International Organization for Standardization (ISO). *ISO 27799-2008 Health informatics — Information security management in health using ISO/IEC 27002*. 2008. Available from: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=41298.

International Organization for Standardization. (2013). *ISO/IEC 2714:2013 Information technology -- Security techniques -- Governance of information security.* Retrieved May 19, 2013 from http://www.iso.org/iso/catalogue_detail.htm?csnumber=43754

Krueger, R.A,. & Casey, M.A. (2009). *Focus Groups*. The Sage Encyclopedia of Qualitative Research Methods. SAGE Publications. Available from: http://0-sageereference.com.library.ecu.edu.au:80/research/Article_n.html.

Mahncke, R.J., & Williams, P.A.H. (2013). Developing and Validating a Healthcare Information Security Governance Framework. *Electronic Journal of Health Informatics* (in press)

McIntyre, A. (2008). *Participatory action research*. Los Angeles : Sage Publications.

Myers, M.D. (2009). *Qualitative research in business & management*. Los Angeles: SAGE Publications Ltd.

National E-Health Transition Authority (NEHTA). (2006). *Review of shared electronic health records standards*. Retrieved April 1, 2006 from http://www.nehta.gov.au/standard-catalogue

National E-Health Transition Authority (NEHTA). *NEHTA releases eHealth information security and access framework to strengthen patient records protection.* 2013 [cited 2013 Feb12]. Available from: http://www.nehta.gov.au/media-centre/nehta-news/942-nehta-releases-ehealth-information-security-and-access-framework-to-strengthen-patient-records-protection

Pharow, P., & Blobel, B. (2004). Security infrastructure services for electronic archives and electronic health records. *Studies In Health Technology And Informatics, 103,* 434-440. Retrieved March 4, 2006 from MEDLINE Database

Royal Australian College of General Practitioners (RACGP). (2005). *Security Guidelines for General Practitioners (February 2005)*. Retrieved June 29, 2009, from http://www.gpcg.org.au/index.php?option=com_content&task=view&id=128&Itemid=38

Schensul, J.J. (2009). *Methods.* The Sage Encyclopedia of Qualitative Research Methods. SAGE Publications. Available from: http://0-sageereference.com.library.ecu.edu.au:80/research/Article_n268.html.

Sharpe, V. A. (2005). *Privacy and security for electronic health records.* The Hastings Center Report. Health Module, 35(6), 3. Retrieved November 5, 2006 from http://www.medscape.com/viewpublication/1164_index

Somekh, B. (2008). *Action Research*. The Sage Encyclopedia of Qualitative Research Methods. SAGE Publications. Available from: http://0-sageereference.com.library.ecu.edu.au:80/research/Article_n4.html.

The Royal Australian College of General Practitioners (RACGP). (2013). *Practice Standards. Computer and information security standards (CISS) 2013*. Retrieved June 30, 2013 from http://www.racgp.org.au/your-practice/standards/ciss.

Williams, P. A. H. (2006a). Security immunisation using basic countermeasures, In H.R. Arabnia and S. Aissi (Eds.), *Proceedings of the SAM'06 - The 2006 International Conference on Security and Management,* (pp.426-432), World Congress in Computer Science, Computer Engineering, and Applied Computing USA.

Williams P.A.H. (2006b). Making research real: Is Action Research a suitable methodology for medical information security investigations?. In C. Valli and A. Woodward (Eds), *Proceedings of the 4th*

Australian Information Security Management Conference, School of Computer and Information Science, Edith Cowan University, Perth, WA. 2006: 184-195.

Williams P.A.H. (2007). *An investigation into information security in general medical practice*. PhD. Edith Cowan University, Faculty of Computing, Health and Science, School of Computer and Information Science. Perth, Western Australia.

Williams, P.A.H. (2013). Information security governance: A risk assessment approach to health information systems protection. In E. Hovenga and H. Grain (eds) *Health information governance in a digital environment.* pp. 186-206. IOS Press: Amsterdam.

Williams, S.P., Hardy, C.A., & Holgate, J.A. (2013). Information security governance practices in critical infrastructure organizations: A socio-technical and institutional logic perspective. *Electronic Markets*, Springer. Retrieved September 29, 2013 from http://link.springer.com/article/10.1007/s12525-013-0137-3