1-1-2011

Help or hindrance: the practicality of applying security standards in healthcare

Patricia A H Williams
Edith Cowan University

DOI: 10.4225/75/57b54c74cd8cd
9th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, 5th -7th December, 2011

HELP OR HINDRANCE: THE PRACTICALITY OF APPLYING SECURITY STANDARDS IN HEALTHCARE

Patricia A H Williams
secau Security Research Centre, Edith Cowan University
trish.williams@ecu.edu.au

Abstract

The protection of patient information is now more important as a national e-health system approaches reality in Australia. The major challenge for health care providers is to understand the importance information security whilst also incorporating effective protection into established workflow and daily activity. Why then, when it is difficult for IT and security professionals to navigate through and apply the myriad of information security standards, do we expect small enterprises such as primary health care providers to also be able to do this. This is an onerous and impractical task without significant assistance. In the development of the new Computer and Information Security Standards (CISS) for Australian General Practice, a consistent and iterative process for the interpretation and application of international standards was used. This involved both the interpretation of the standards and the application of knowledge to create a practical but acceptable level of security for the primary healthcare environment. From a security perspective such practical application of standards poses the dichotomous challenge (and criticism) of how much security is sufficient versus how much can the primary healthcare environment manage. This paper describes the path of development from standards to implementation using the CISS as an example. It is concluded that more practical assistance is required by the security profession to support the national e-health initiative if Australia is to provide a safe and secure healthcare environment.

Keywords
Information security, standards, medical, healthcare security.

INTRODUCTION

A national e-health system for Australia is rapidly becoming a reality. The political drive for a Personally Controlled Electronic Health record (PCEHR) has seen the rapid progression of the underlying e-health infrastructure. The PCEHR will provide a “secure, electronic record of your medical history, stored and shared in a network of connected systems. The PCEHR will bring key health information from a number of different systems together and present it in a single view” (NEHTA, 2011). This is not designed to replace the complete patient record held at the local medical practitioner but to provide a collated view of the patient health summary that will be able to be shared with other health providers. As such, the PCEHR is not of itself the basis for the e-health system; it is only one part of it. Thus the protection of patient information is now more important as a national e-health system approaches reality in Australia. The major challenge for health care providers is to understand the importance information security whilst also incorporating effective protection into established workflow and daily activity.

The development of a coherent and interoperable e-health system in Australia is made more complicated by the division of control between the federal (national) and state governments for public healthcare services as well as the strong private healthcare sector in the primarily private primary care sector, and some allied and hospital services. Therefore, information security protection for smaller healthcare providers, such as those in general practice, is particularly important and the focus of this paper. At the heart of creating an infrastructure that supports information sharing are standards to ensure interoperability and consistent information management. Information security is an integral part of this architecture. Since information security is an established and well developed discipline, the existing mature practices are a key component of this architecture. Why then, when it is difficult for IT and security professionals to navigate through and apply the myriad of information security standards, do we expect small enterprises such as primary health care providers to also be able to do this.

Standards, policies and recognized practice do not need to be redeveloped for the healthcare environment. However, there is no doubt that they do need to be contextualised and modelled to fit into a well established health framework, rather than attempting to cascade over and impose a regime of security (as is the case in the corporate environment) that so obviously does not fit well into the healthcare setting . This paper discusses the standards that are relevant to the primary healthcare setting and provide a case study of how these can be interpreted and applied. This development has been an integral part of the development of the new Royal

Australian College of General Practitioners, Computer and Information Security Standards, and the paper gives this as an example of what work is needed in this area.

SECURITY STANDARDS FOR HEALTHCARE

Established and accepted information security management planning includes, risk assessment, contingency planning (business impact analysis, incident response, disaster recovery and business continuity) and protection controls and monitoring (Whilman & Mattord, 2008). In the security community it is widely accepted that standards must drive policy which then informs decision making and good security practice.

The application of standards is not an insignificant task. "One of the great challenges facing IT professionals is how to navigate through the sea of regulatory compliances, industry standards, and numerous security and IT operational best practice standards and frameworks" (Tordoff, 2008). Further, complexity is apparent in that standards tend to focus on process rather than application and implementation. Indeed, it is not surprising that standards must be contextualised to synergise with an organisation's culture, support its mission and fit into established work processes (Hone & Eloff, 2002).

All organizations have multiple legislative regulations to comply with, and healthcare has the added professional and ethical requirements inherent to the environment. What is required for demonstrable defensible practice are cohesive and realistically implementable information security plans that can be assessed and measured for protection compliance, and can be used as a guide for improvement. It must be accepted that information security is always going to be a 'work in progress' and that 100% security is rarely, if ever, achievable; indeed, some would argue that it is impossible to achieve. For instance, hacking is a sophisticated attack mechanism and therefore unpredictable and difficult to prevent. In the USA, breach notification legalisation in enacted which provides some measure of the enormity of the problems now being encountered in regards to breaches from malicious and human error (Hancock, 2005).

The problems with security standards application

The major challenge for health care providers is to understand the importance of information security whilst also incorporating effective protection into established workflow and daily activity. This is an onerous and impractical task without significant assistance. This challenge does not only reside with the healthcare profession and those in the context to which the standards are applied, but also for the security profession and the standards community who advise and set the standards. They also need to understand a broader perspective on the realistic application of these standards. Indeed, even the standards community recognize that applying standards needs contextualization, as is evidenced by the development of ISO27799 from ISO27002. Table 1 shows the standards that are directly relevant to the development of practical information security guidance in the primary healthcare setting.

Standards exist to ensure a secure system and provide associated minimum technical specifications. It is therefore necessary to translate a standard into policy and then procedures specific to the environment of use. Yet, this has been problematic in the healthcare environment. Policy derived from standards must be singular and continually monitored if it is to be effective (Owens et al, 2001). The real and perceived cost overhead, which whilst reducing risk and contributing to information protection does not overtly contribute to patient care simply adds to the misunderstanding of the importance of security at the management level. To date whilst quoting risk assessment as an integral part of security, it is an task that is not really assessed, whether from being too difficult or time consuming to be undertaken, and its omission limits both the understanding of the issues and the importance of what realistically needs protection. Whilst the Australian HB 174-2003 handbook features best practice control measures for information security and is designed for a non-technical readership, it does not alone assist in implementation application. Similar to other guidelines, it does not cater for specific types of health providers or organisations and therefore contains a more complicated picture for those with minimal security knowledge.

The issue with using un-interpreted standards is the level of knowledge and expertise that is required to apply and implement them, the resourcing that is often associated with this in terms of time, and the impetus to undertake the task. In the healthcare environment this issue has been evident from research and experience in the field (Williams, 2008). The autonomous nature of staff in healthcare and specifically in smaller healthcare organisations reinforces informal and individualised work practices. This can be a barrier where a lack of fit between policy and work practice occurs (Adams and Blandford, 2005). Part of the problem is to create a culture around the integration and recognition of security in the work place. This however will always be a challenge in an environment that is not corporately based and where security is not considered integral to core business. However, where treating patients and healthcare are the main focus, the correct and protective management of healthcare information is essential, particularly as the connectedness of the e-health environment is gradually put in place. The following section outlines how development of a minimised and simplified process using the relevant standards in Table 1 has been achieved with the 2011 Royal Australian College of General Practitioners (RACGP) Computer and Information Security Standards (RACGP, 2011).

Standard	*Description*	*Relevance to the application to general practice*
ISO/IEC 27001:2005 - Information technology -- Security techniques -- Information security management systems -- Requirements.	*General business implementation not tailored for healthcare. Part of the ISO 27000 group of standards for Information Security Management Systems*	*Incorporates basic processes for risk assessment and identification of overarching principles.*
ISO 27002 (previously ISO 17799:2005) Information technology - Security techniques - Code of practice for information security management	*Developed from ISO/IEC 17799:2000. It provides best practice guidelines for Information Security Management Systems implementation.*	*Provides detailed areas of security with background explanation of importance. It also provides some (but not all) indication of technical and social measures required in general principle form.*
ISO 27799-(Health informatics - information security management in health using ISO/IEC 27002	*Applied the context for using ISO 27002 to healthcare setting in general and incorporates aspects of interoperability considerations.*	*Whilst incorporates controls these are not prioritized. They were referred to complete parts of the matrix for risk assessment and controls once the categorization and prioritization of risks were established.*
HB 174-2003- Information security management - Implementation guide for the health sector	*This handbook was derived from NZS ISO/IEC 17799:2001 and details the controls specifically for the health sector in Australia.*	*This provided grounding in the application for the Australian scenario. Whilst aimed at small to medium enterprises it still does not embrace the difficulties faced by primary care practices in lack of IT and security expertise, It is also now out of date in some areas.*
ISO 31000:2009 Risk management – principles and guidelines.	*Provides generic guidance on risk principles.*	*Used to ensure comprehensive coverage of risk issues.*
HB 231 - 2004 Information security risk management guidelines.	Generic guidance on implementation of a risk management process.	*Used in conjunction with ISO31000 to provide the practical aspects and determine to what extent these applied to the primary care environment.*
HB 292 - 2006 A practitioners guide to business continuity management; and HB 293 - 2006 Executive guide to business continuity management.	*Provides generic but accepted and integrated approach to business continuity in the business and corporate environments.*	*Used specifically to inform the development of the business continuity section.*
Guidelines contributing to the Australian primary care information protection principles • Information Privacy Principles under the Privacy Act 1988 • NIST (2008). Computer security incident handling guide. Special Publication 800-61. National Institute of Standards and Technology. • Office of the Australian Information Commissioner. (2006). National Privacy Principles		

Table 1. Standards relevant to development of practical guidance to primary care in information security.

CASE STUDY IN APPLICATION TO HEALTHCARE

In the development of the new Computer and Information Security Standards for Australian General Practice, a systematic process for the analysis and application of international standards was used. This involved both the interpretation of the standards and the application of knowledge to create a practical but acceptable level of security for the primary healthcare environment. The process was systematic as each standard was reviewed in order and used to inform the development of the major risk-control matrix shown in Table 2.

As in many specific areas of healthcare and business for small organisations, it is the time and expertise factors that interfere with the development of good practice in security. With this in mind, it was necessary to use the authors' experience and knowledge of both the security and healthcare areas to formulate a simplified but effective process for ensuring good security practice and protection in general practices. For this objective the standards in Table 1 were systematically reviewed and used to guide this development, whilst consistently applying the knowledge of what was possible and practical for practices to undertake themselves. Table 2 indicates the synthesis of this into a simplified form. Table 2 is an extract only of the full table in the published RACGP Computer and Information Security Standards Workbook (RACGP, 2011), and in the published version each dot point is also cross-referenced to the RACGP Standard for further explanation.

It should be noted that this is not the whole process and other aspects integral to the management of the information security process were also included, such as establishing responsibilities, contact points, asset identification etc, However, these are not provided here for the purpose of this case study. What was required was to identify the common threats to the primary care environment and provide associated mitigations without making the requirements is large a task that it would not be undertaken at all and therefore not useful. The selection of threats also included link to the privacy principles as well as the ethical and professional aspects of clinical practice and the protection of patient information.

Risk Assessment – Threat, vulnerability and controls						
Threat / Risk Source	***Disruption / Impact***	***Vulnerability***	***Suggested Appropriate Controls***	***Controls***		***Person Responsible***
				Existing	***Required (to action)***	
Human – Unintentional- – Internal (insider threats/staff/authorised third parties)						
Error / omissions e.g. deletion of files, failure to check backup	- Financial loss - Disrupt operational activities -Breach of integrity (inadvertent information modification or destruction)	- Legitimate access to systems - Lack of training	Staff training in policy and procedures Backup and recovery procedures in place	*<practice to complete>*	*<practice to complete>*	*<practice to complete>*
Inadvertent access by staff	- Violation of legislation or regulation - Breach of confidentiality (potential information disclosure)	- Legitimate access to systems by staff - Lack of formal implemented policy and procedures, particularly password controls	Implemented and monitored access control policy and procedure Breach reporting in place Confidentiality and non-disclosure agreements signed Agreements with third parties signed Password protected screen savers Limit access to system utilities			
Inadvertent viewing of information by non-staff	- Violation of legislation or regulation - Breach of confidentiality	- Lack of appropriate access control - Staff not following policy	Staff training in policy and procedures Clear desk and clear screen policy			

Risk Assessment – Threat, vulnerability and controls						
Threat / Risk Source	***Disruption / Impact***	***Vulnerability***	***Suggested Appropriate Controls***	***Controls***		***Person Responsible***
				Existing	***Required (to action)***	
Technical – Deliberate						
Malicious code (e.g. virus)	- Disrupt operational activities - Denial or degradation of service - Data loss - Breach of integrity	- Inadequate network and internet protection - Lack of staff training -Not keeping anti-virus updates current - Spam filtering	Anti-malware software automatically regularly updated Regular precautionary scans of information systems Spam filtering Staff education on email attachments Prohibit use of unauthorised software Block use of mobile code e.g. use web browser security to limit program add-ons (unknown ActiveX) Limit use of file transfer/peer-to-peer applications unless essential to normal operations Control or prohibit use of external and personal devices such as USB			
Information loss	- Violation of legislation or regulation - Adversely affect reputation - Breach of confidentiality	- Poor or no backup procedures - Lack of appropriate access control	Effective, monitored backup procedures Breach reporting to authorities Segregation of system utilities from application software (seek advice from technical service provider). Limit access to system utilities			
Denial of Service (DoS - attempt to make computer resources unavailable)	- Loss or degradation of network capacity - Loss of Internet connectivity		Configure Intrusion detection system to detect DoS Firewall configuration to block specified network traffic Block outgoing connections to Internet relay chat (IRC), instant messaging and peer-to-peer services(seek advice from technical service provider)			

Table 2. Threats, vulnerabilities and controls for general practice security (RACGP, 2011, extract of Table 22)

Whilst only an abstract of the matrix is given in Table 2, the full matrix includes the six categories of

- Human – Unintentional- – Internal (insider threats/staff/authorised third parties)
- Human – Deliberate – Internal (insider threats/staff/authorised third parties)
- Human – Deliberate – External
- Technical – Unintentional
- Technical – Deliberate
- Environmental

It is clear that most explicit environments and domains have specific security threats and vulnerabilities, and as such the majority of the risk and control matrix can be completed by those knowledgeable of security and the specific domain to which it is being applied. Therefore the whole process of implementing security can be made more straightforward. Subsequently, a medical practice can record the existing measures they already have in place and identify easily those that need to be considered. This can be done to a greater extent without the assistance of external support providers in the first instance, although the matrix does identify when this assistance may be required.

In a similar development manner, the business continuity section of the workbook (deemed to be an area of major concern to the profession and poorly executed in many general practices) was also developed to assist practices in indentifying their critical functions, manual or replacement procedures in the event of the system failure, and corrective actions using simple tables to both create and define logical procedures. The standards and workbook were reviewed and validated by other experts in the security and healthcare field, the RACGP e-health unit, general practitioners, practice managers, as well as the National Standing Committee for E-Health.

CONCLUSION

From a security perspective, the practical application of standards poses the dichotomous challenge (and criticism) of how much security is sufficient versus how much can the primary healthcare environment manage. The recent development of the RACGP Computer and Information Security Standards and Workbook has taken six months of interpretation and application of the standards. They demonstrate that practical assistance can be developed in such as way to assist primary care practices to put in place sufficient and effective security measures. This standard will now be incorporated into the RACGP national accreditation of general practice and will provide evidence of a basic level of security practice by healthcare providers. For medical practices it will also offer a method for demonstrable practice and guidance in improvement in practice as some aspects are aspirational. To the healthcare profession it indicates the importance of information security in understandable terms, and provides a basis for the extension of security measures that will be necessary for connection to the national e-health system which (driven by the political landscape) will begin in earnest in July 2012. It is intended that this RACGP standard will be extended to incorporate all office based medical practices in 2012.

The security profession must work together with the healthcare profession to provide both technical expertise and increased social awareness of the importance of information security. Whilst this may not be a necessity peculiar to the healthcare domain, it is proving a challenge in the current progressive e-health environment. It is highly likely that the perception of information security and its importance will develop as the e-health information sharing situation evolves in Australia over the next few years. Whilst some of this may be driven by legislation and the altered information sharing environment shifts, this perception will not occur automatically. Ultimately, it will require a change of healthcare organisational culture to reframe the importance and significance of information security to the e-health environment.

REFERENCES

Adams, A. and Blandford, A. (2005). Bridging the gap between organizational and user perspectives of security in the clinical domain. *International Journal of Human-Computer Studies, 63* (1-2), 175-202.

Hancock, E. (2005). Over 50 million served....and counting: The scope of liability and legal duty for data breaches. Journal of Internet Law, 9 (2), 1 & 13-24.

Hone, K. And Eloff, J.H.P. (2002). Information security policy – what do international information security standards say? *Computers & Security 21* (5), 402-409.

King, S. (2004). Applying application security standards – a case study. *Computers & Security 23*(1), 17-21.

NEHTA. (2011). *What is a PCEHR?* Retrieved from http://www.nehta.gov.au/ehealth-implementation/what-is-a-pcher

RACGP. (2011). *Computer and information security standards and workbook.* Melbourne, Australia: Royal Australian College of General Practitioners. Available from http://www.racgp.org.au/ehealth/ciss

T. J. Owens, S. Tachakra, K. A. Banitsas, and R. S. H. Istepanian, (2001). Security a medical wireless LAN system. *Proceedings of the 23rd Annual EMBS International Conference*, Istanbul, Turkey, pp. 3552-3555.

Tordoff, M. (2008). Applying Security Standards Like ISO 27002 to Compliance Requirements. Retrieved from http://it.toolbox.com/blogs/security-compliance/applying-security-standards-like-iso-27002-to-compliance-requirements-22446.

Whitman, M.E. and Mattord, H.J. (2008). *Management of information security (2nd Ed.)*. Australia: Thomson Course Technology.

Williams, P.A.H. (2008). When trust defies common security sense. *Health Informatics Journal,14*(3), 211-221.