2013

Ehealth Security Australia: The Solution Lies with Frameworks and Standards

Bryan Foster
National E-Health Transition Authority (NEHTA), Byron.Foster@nehta.gov.au

Yvette Lejins
National E-Health Transition Authority (NEHTA), Yvette.Lejins@nehta.gov.au

DOI: 10.4225/75/579810e331b3e
Originally published in the Proceedings of the 2nd Australian eHealth Informatics and Security Conference, held on the 2nd-4th December, 2013 at Edith Cowan University, Perth, Western Australia

EHEALTH SECURITY AUSTRALIA: THE SOLUTION LIES WITH FRAMEWORKS AND STANDARDS

[1]Byron Foster, [2]Yvette Lejins
National E-Health Transition Authority (NEHTA)
[1]Byron.Foster@nehta.gov.au, [2]Yvette.Lejins@nehta.gov.au

Abstract

Security is a key foundation for eHealth in Australia, driving benefits in healthcare quality, safety, and efficiency towards improved health outcomes for all Australians. To this end, the National eHealth Transition Authority (NEHTA), the Royal Australian College of General Practitioners (RACGP), and Standards Australia have each produced security-related publications to assist Australian healthcare organisations protect their data. These publications provide standards, tools, and guides for the healthcare industry to build and implement secure systems that protect patient data and eHealth-related assets, while providing the provenance required to help ensure patient safety and privacy. This paper outlines some of the current and emerging threats and risks to eHealth in Australia, and how these Australian security-based standards and frameworks can assist in mitigating such threats, support the management of information security risks, and maintain legislative compliance.

Keywords
eHealth Security, National eHealth Security and Access Framework, PCEHR, Computer Information Security Standards, National eHealth System, HB174.

INTRODUCTION

Australia's national eHealth system is gaining momentum and increasingly being embraced by both practitioners and consumers alike. The considerable investment in Australia's national eHealth program has led to, and will continue to produce, major changes to the ways in which health organisations and practitioners provide healthcare. As reported in the NEHTA 2012 /2013 annual report (NEHTA, 2013), as of September 2013 over 900,000 Australians registered for a National eHealth Record, known as a Personally Controlled Electronic Health Record (PCEHR). Furthermore, over 13,000 health practitioners and healthcare organisation have registered and received a National Authentication Service for Health (NASH) digital token to both identify and authenticate to eHealth national systems as well as to allow point-to-point authentication between providers and healthcare organisations. Health practitioners are starting to reap the benefits from these investments in eHealth to be able to facilitate patient healthcare and to communicate securely between providers.

Crucial to the ongoing increased adoption and uptake of these eHealth systems is the important concept of trust. Successful eHealth initiatives around the world rely on patients and healthcare professionals trusting in the information systems and solutions they use. This trust stems from people having confidence in the system's content; in their ability to appropriately access, collect, use, disclose, and update healthcare information held by these systems; and in the knowledge that the data is held privately, in line with patient wishes and clinical needs. Healthcare organisations face increasing challenges when managing health information risks across the enterprise, and between organisations.

The connected healthcare system provides a rich breeding ground for risks to individual privacy, confidential information, data integrity, and service availability. As a result, participating organisations must examine ways to address those challenges when making security arrangements, both physically and logically. As more health organisations and practitioners participating in eHealth, and interconnect with eHealth systems, there is an increased need for pragmatism about the security risks, and for such organisations to seek out guidance on what is required to protect the sensitive information in their custody. The challenge confronting most healthcare organisations is balancing security compliance, and the enforcement of risk controls, with improved patient outcomes. While the security of patient information and the systems that store, access and exchange this information may appear to be secondary to the core business of facilitating patient care, ensuring an operationally realistic balance between security and patient care should be a key driver.

Robust security practices and processes are required to meet legal obligations and protect personal health information. While organisations have had to comply with Federal and State Privacy Acts for many years, upcoming amendments to the Privacy Act introducing the new Australian Privacy Principles (OAIC, 2013), that come in to effect in March 2014, include heightened security requirements. In addition, organisations using

national eHealth systems need to be cognisant of their responsibilities under the Healthcare Identifier Act 2010 (The Health Identifiers Act, 2010) and Personally Controlled Electronic Health Record 2012 Act (PCEHR, 2012). While the ultimate driver for information protection and security should be because it is the 'right thing to do', healthcare organisations and those that access health information are required to take reasonable steps to protect health information. For some, these reasonable steps may not instigate great managerial or technological change or be overly onerous, but for many there needs to be an examination and change to the configuration of their technology, policy, practices, and process so as to limit their exposure.

Besides changes to legislation requiring individual and organisational compliance, there has been a significant shift in the threat and risk landscape. Key findings from the PwC Global State of Information Security Survey 2014 (released October 2013) (PWC, 2013) indicate that the number of security incidents globally detected by healthcare providers in the last 12 months has increased by 39%. Interpreting this data can lead to two main, possible conclusions. The first conclusion being that security incidents have increased because more sophisticated detection mechanisms have been implemented, given there is better technology, policies, processes in place for health organisations. The second is that security attacks and incidents are simply on the increase. It is probable that it is a mixture of the two – the increased implementation of better detection capabilities, coupled with an increase in incidents. Interestingly, the same survey found that 74% of healthcare provider respondents believe their security activities are effective.

This paper outlines some of the current security threats and risks to eHealth in Australia, and outlines how the National eHealth Security and Access Framework (NESAF) (NEHTA, 2012) and other Australian security based standards, can assist in mitigating these threats by laying effective foundations.

EHEALTH AND THE THREAT LANDSCAPE

Information security and the requirements for health provider organisations are unique, when compared to other industries. Health provider organisations are at a crossroads to provide better and more effective patient care while ensuring confidence and trust in the systems used in its provision.

The eHealth landscape is also exciting, and offers new opportunities to access life-saving information in a more timely fashion. There is perhaps no other industry sector where the information that is collected and used is so sensitive, and requires such rigour so as to ensure that the security controls implemented will ensure that privacy obligations and assurances will be met.

The threat landscape is evolving and morphing as new threats are identified daily, increasing the risks to the information that healthcare provider organisations hold and exchange. Industry has observed interesting and 'clever' developments resulting in some high profile security incidents that are reported widely by the media. As health sector participants become more interconnected, the vectors for exploitation increase, and the risks heighten, with increased 'pain points' for businesses to now identify and protect. This, coupled with the increased volume of electronic data flows between health organisations, an increased number of national systems and repositories also means that the traditional boundaries requiring protection have eroded and can be difficult to identify. Furthermore, the participation of vendors, suppliers, (and the greater use of cloud providers) who may be custodians to proprietary systems and data stores only compounds the problem of safeguarding the end-to-end environment.

The introduction of emerging technologies like bring your own device (BYOD), Cloud Computing and mobile application development within healthcare provider organisations has provided great benefits, but they also expose the organisation to more threats and increased risks. Additionally, there is a lack of targeted advice specific to healthcare that can be used to manage these problems. Often the risks of uptake and use of these technologies is not appropriately explored and assessed prior to deployment.

Risks to the healthcare provider organisation embarking on the use of these emerging technologies come primarily from the mobile nature of the technology, and the possibility that parts of the solution may not be under the control of the organisation. Risks can range from untrusted unsecured devices with access to patient data, or mobile applications not developed with security considerations, to the storage of health data on cloud services or mobile devices connected to untrusted networks or Wi-Fi hotspots. Healthcare practitioners need to be aware of these risks and provide services that are secure and make use of equipment and software appropriately. Healthcare provider organisations should ensure that they understand the additional risks that these technologies impose on their organisations, and include these technologies as part of their overall security program.

Recently the Australian Broadcasting Corporation news and IT magazine "Pulse" have published instances where , the threat of 'ransomware' has been felt on a number of small Australian health organisations, such that these organisations have been held ransom by attackers who have encrypted the contents of patient databases and extorted the organisation for compensation to decrypt the data (ABC News, 2012; McDonald, 2012). Ransomware may not just be encryption of data but may also involve malware programs loaded onto systems that deny access to various types of information.

To date, there have been more than 30 "ransomware" attacks reported in Australia, and more than 20.000 attempted attacks a day are estimated to take place in Europe according to the ABC report (ABC News, 2012). The targets of these attacks have tended to be smaller businesses without the knowledge or expertise to implement the required security controls to mitigate against these attacks; but no organisation is exempt from such attempts. Without the guidance of a framework or security program to help these organisations address security, these attacks vectors may become more predominant.

Phishing, while not a new threat, is one that has managed to evolve in becoming more sophisticated and more recently being targeted at specific individuals or companies, and termed 'Spear Phishing'. Either attempt are, in most instances, carried out through email or instant messaging technologies by requiring the recipient to open a link within the email message to a fraudulent website. Malware is then used to obtain personal information from the recipient, including usernames, passwords, and banking information.

Healthcare provider organisations' security policies and awareness training need to address the use of electronic communication within the organisation, and users should be made aware of the risks of social media sites, instant messaging, and email technologies. Healthcare organisations should encourage staff not to open messages from untrusted sources, and report any suspicions communications that may be malicious.

A persisting misconception is that if an organisation invests in technology, and protects its perimeter through technology, that it is secure and not susceptible to any threats or risks, however, this has proved not to be the case. Healthcare provider organisations forget about the 'people and process factor', and fail to provide staff with the awareness to identify threats, or the policy to address them. Consequently, thorough policies and procedures are necessary to ensure against abuse, provide safeguards, ensure adequate remedies, and make sure these protections are enforceable.

Healthcare provider organisations should effectively communicate security awareness to appropriate audiences. Awareness training, and intra-organisational communication, is an essential component in any security programme. Organisations must train their staff to be vigilant and aware. However, no matter how well trained staff may be, or how aware they might be, it is a numbers game. Eventually they will fail. Consistently, people prove that they are an easy target for social engineers to target and exploit.

Certain industries and sectors in Australia are regulated and require protection of information to a set of required security controls set down by an overseeing body. For example, collecting credit card information requires familiarity with the Payment Card Industry Data Security Standard (PCI DSS). Systems maintained by the Australian federal government may require certification and accreditation to the Information Security Manual (ISM), and Protective Security Policy Framework (PSPF), (as was undertaken for the PCEHR National Infrastructure, the Health Identifiers and NASH Services). In absence of health specific regulations, many organisations adopt ISO/IEC 27001 as a best practice security management framework and certify to it.

There are unique controls and additional considerations required in the protection of private and personal health information. While specific legislation does touch on security controls required, there is no specific security compliance regime that exists in Australia for healthcare.

However, the following legislation in Australia is directly relevant to healthcare organisations, depending on jurisdiction and the use of eHealth information will drive what you need to comply to:

- Health and Privacy legislation relevant to your individual state or territory;
- The Privacy Act 1988 (Cwlth) (Noting an amendment to the Privacy Act introducing the new Australian Privacy Principles to be introduced in March 2014, containing significant changes to requirements for the protection of information);
- The Healthcare Identifiers Act 2010 (Cwlth); and
- Personally Controlled Electronic Health Records Act 2012 (Cwlth).

Unfortunately, legislation alone does not provide the analysis, or understanding of an organisation's unique risk profile to afford all the specific guidance an organisation may need. This is where Australian security frameworks and standards developed in Australia need to be examined and applied to a healthcare organisation, as relevant. Application of some of these standards can assist in ensuring that healthcare organisation are secure and that healthcare providers are fulfilling security obligations as outlined in the PCEHR, HI Service, and Privacy acts

WHAT HAS BEEN DEVELOPED TO ASSIST HEALTHCARE ORGANISATIONS?

To date, healthcare industry experts and standards bodies have developed publications that guide the healthcare community in implementing efficient and effective security programs. Implementing these standards or frameworks will assist in mitigating identified threats and risks, Three main publications have been drafted:

- **NESAF:** The National eHealth Security and Access Framework (NESAF) version 3.1, developed and published by the National eHealth Transition Authority (NEHTA) in 2012, but version 4.0 due for publication by the end of 2014;
- **CISS**: The Computer Information Security Standards (CISS), 2nd edition published by the Royal College of General Practitioners (RACGP) in 2013; and
- **HB174**: AS/NZS HB174:2003 Health information security implementation guide for small and medium businesses, published by Standards Australia in 2003.

Each publication focuses on providing guidance to distinct healthcare industries, but each is complementary in the guidance it offers and can be implemented into any healthcare setting. The CISS has been designed to specifically target general practices, while the NESAF is designed to be scalable to any healthcare organisation, regardless of size, and considers security more holistically than just the organisation applying the framework. HB174 is geared towards those smaller healthcare providers that may have limited security capability and need a starting point.

Computer Information Security Standards (CISS)

The recently updated and published Computer Information Security Standards (CISS) provide detailed guidance for general practices, with advice specifically targeted for that community. Consequently, although other organisations can look to it as a source of contemporary and relevant information, it may not fulfil all their unique security needs.

The CISS provides general practices with a framework for evaluating risks, guidance, and solutions to improve competency and capacity in computer and information security, and uses a maturity model to establish the relative maturity of the practise under review. It also assists GPs and their practice teams develop policies for appropriate participation with the PCEHR.

The CISS are comprised of the following:

- **A compliance checklist,** designed to help practices determine whether reasonable computer and information security measures have been established and maintained to protect the security of clinical and business information, on an ongoing basis;
- **Twelve computer and information security standards**, each of which contains:
    - A user-friendly compliance indicator matrix; and
    - Explanatory notes for each compliance indicator, designed to explain each standard, and the actions required to minimise potential risks to computer and information systems.
- **Additional templates,** consisting of sample tables and forms to assist practices to develop and record their own policies and procedures for computer and information security.

The standards align with relevant legislation, including the Privacy Act, the National Privacy Principles, the Healthcare Identifiers Act, and the Personally Controlled Electronic Health Records Act.

Australian Standards HB174 Handbook

HB 174 published by Standards Australia (2003), targeted towards small and medium healthcare organisations to assist them in aligning to the ISO/IEC 27001 information security management standard. The handbook covers all key control areas of the standard, except for system development and maintenance. Unlike publications such as the NESAF, HB174 is more organisation-centric, and does not address the exchange and journey of information as it transitions through the healthcare system.

The Handbook published in 2003, and its age means that specific areas such as cloud computing, ransomware, and even wireless technology have not explored. Australian eHealth was in its infancy, so national electronic health records (such as the PCEHR) were not yet established. Notwithstanding, HB174 is still somewhat 'technology proof' and 'technology agnostic'. The underlying principles for best practice security management have not changed over time, and this handbook has provided an important source of targeted and industry specific security information for the health sector in Australia.

National eHealth Security and Access Framework (NESAF)

The NESAF, published by NEHTA, designed to assist all healthcare organisations, regardless of size, or complexity of their eHealth exchanges, The NESAF document suite provides the most comprehensive coverage of security and access guidance for the Australian health sector. The NESAF has been developed in collaboration with almost 200 unique stakeholders, including health practitioners, health business owners, health information managers, consumers, privacy advocates, information security experts and health technology specialists. The NESAF starts by focusing and understanding the risk profile of a given organisation, and where it will be located in the overall eHealth environment.

In short, the NESAF provides:

- Scalability to address the future state for eHealth in Australia;
- Focus on outward and exchange, journey, and provenance of information – rather than just organisation-centric)
- An Australian-specific focus, in relation to health security issues.
- Healthcare-specific process patterns to help identify and classify healthcare information
- Information on specific legislation, such as Commonwealth and State privacy laws, the Healthcare Identifiers and PCEHR Acts.

The core framework of the NESAF includes:

- A **set of principles** that are intended to guide the design and implementation of secure eHealth systems;
- A **framework model** that identifies key security and access control areas, control objectives, and controls;
- A **risk-based approach** to support implementation of the framework, including a gap analysis and risk assessment tool that organisations can use to assess their level of risk and compliance with each of the security and access control areas within the framework model; and
- A **toolkit** that provides a comprehensive library of information relevant to specific eHealth processes, with security and access functions. Key components of the toolkit include:
    - eHealth process patterns that assist business to identify core security and access functions in context of their business;
    - A reference library of process patterns, security, and access functions;
    - Service descriptions that include relevant standards, controls, better practice examples, compliance, services, policy, and identify issues associated with each security and access function; and
    - The core principles of the NESAF, which is intended to guide the application of the framework in the design and implementation of secure eHealth systems to manage and protect healthcare information.

The NESAF has been providing healthcare organisations with the necessary information and guidance to assist in ensuring that their systems are secure and fulfil security obligations as outlined in the PCEHR, HI Service, and Privacy Acts.

Depending on the type of healthcare organisation and the business it undertakes, will drive what is the most appropriate security standard or framework to adopt. Notwithstanding, there will be elements of each of the frameworks that will resonate with an organisation to ensure that the most appropriate security controls are identified and subsequently applied. In the Australian ehealth ecosystem, and integration into the national ehealth system means that not implementing a security program is not an option. It is not just about protecting the information an organisation is custodian too, but now there is a larger number of parties having access to national information stores and involved in the exchange of sensitive information that needs appropriate protection. Australian healthcare organisations should be prepared to implement better security for their systems, by adopting a framework or standard that will assist in enhancing clinical safety and privacy obligations.

CONCLUSION

The delivery of eHealth in Australia is culminating in a surge of personal healthcare data bought online by heterogeneous organisations. Emerging technologies such as cloud computing, mobile applications, and 'big data' are helping to drive the delivery of this information. Although the potential benefits for patient care delivery are enormous, healthcare organisations need to understand their responsibilities and obligations, and be vigilant regarding the additional risk imposed on their organisation.

Information security and privacy policy are critical in supporting confidence in eHealth products and solutions, medical technology, and the electronic exchange and storage of health information. Organisations need to instil a pervasive culture of security amongst their staff when safeguarding health information data if they are to avoid becoming the weakest link in the national eHealth system.

Health organisations should approach security in a strategic, thoughtful, and well-planned manner; the application of an appropriate security standard or framework is therefore imperative. There is no one-size-fits-all approach, nor is there a checklist of activities to complete. Rather, each health provider organisation should specifically tailor its security program, policies, and practices to meet its business needs and address its unique data security risks and vulnerabilities.

REFERENCES

ABC News. (2012). *Ransomware targeting businesses, home PCs*. Retrieved from http://www.abc.net.au/news/2012-10-25/ransomware-targeting-aussie-businesses2c-pcs/4332526

Computer Information Security Standards (CISS). (2013).Retrieved from http://www.racgp.org.au/your-practice/standards/computer-and-information-security-standards

McDonald, K. (2012). South Australia new target for Ransomware attacks. *Pulseit Magazine*,12 Dec,2012. Retrieved from http://www.pulseitmagazine.com.au/index.php?option=com_content&view=article&id=1256:south-australia-new-target-of-ransomware-attackers&catid=16:australian-ehealth&Itemid=328

NEHTA (2012) *National eHealth Security and Access Framework (NESAF).*

Retrieved from http://www.nehta.gov.au/implementation-resources/ehealth-foundations/EP-1005-2012/NEHTA-1006-2012

Retrieved from http://www.nehta.gov.au/implementation-resources/ehealth-foundations/EP-1005-2012/NEHTA-1008-2012

Retrieved from http://www.nehta.gov.au/implementation-resources/ehealth-foundations/EP-1005-2012/NEHTA-1004-2012

Retrieved from http://www.nehta.gov.au/implementation-resources/ehealth-foundations/EP-1005-2012/NEHTA-1010-2012

Retrieved from http://www.nehta.gov.au/implementation-resources/ehealth-foundations/EP-1005-2012/NEHTA-1007-2012

Retrieved from http://www.nehta.gov.au/media-centre/news/publications/brochures/299-national-ehealth-security-and-access-framework-consumer

Retrieved from http://www.nehta.gov.au/media-centre/news/publications/brochures/300-national-ehealth-security-and-access-framework-clinical

Retrieved from http://www.nehta.gov.au/media-centre/news/publications/brochures/301-national-ehealth-security-and-access-framework-business

NEHTA. (2013). *September 2013 annual report*. Retrieved from http://www.nehta.gov.au/media-centre/news/470-nehta-s-annual-report-2012-13-is-now-available

OAIC. (2013). *Australian Privacy Principles*. Retrieved from http://www.oaic.gov.au/privacy/privacy-act/privacy-law-reform

PCEHR. (2012). *Personally Controlled Electronic Health Records Act 2012.* Retrieved from http://www.comlaw.gov.au/Details/C2012A00063

Privacy Act 1988. Retrieved from http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/

PWC. (2013). *PricewaterhouseCoopers Global State of Information Security Survey 2014* Retrieved from http://www.pwc.com.au/consulting/publications/global-information-security/index.htm

Standards Australia. (2003). *Information Security Management – Implementation guide for the Health Sector (HB174).* Retrieved from http://infostore.saiglobal.com/store/details.aspx?ProductID=568742

The Healthcare Identifiers Act 2010. (2010). Retrieved from http://www.comlaw.gov.au/Details/C2010C00440