Does the PCEHR mean a new paradigm for information security? Implications for health information management

Patricia A.H. Williams

Abstract

Australia is stepping up to the new e-health environment. With this comes new legislation and new demands on information security. The expanded functionality of e-health and the increased legislative requirements, coupled with new uses of technology, means that enhancement of existing security practice will be necessary. This paper analyses the new operating environment for Australian healthcare and the legislation governing it, and highlights the changes that are required to meet this new context. Individuals are now more responsible for security and organisations should be prompted to review their security measures in light of the new demands of legislative compliance.

Keywords: *Computer Security; Medical Informatics; Health Information Systems; Computer Security; Electronic Health Records.*

Introduction

It is important to ensure appropriate protection of health information and demonstrate clinical utility if Australia's new e-health system and personally-controlled electronic record (PCEHR) is to be successful. Good security measures are required not only to protect personal information, but also to meet new and existing legislative requirements. Further, the PCEHR development has been informed by international standards across the clinical, data transmission and security domains, which provides a grounding to achieve longer term success in e-health (NEHTA 2010, 2011a, 2011b). This development has been extended to establish Australian standards to reflect the development of the e-health system and the PCEHR in the Australian environment (NEHTA 2013).

The context for e-health differs from existing health records systems as it broadens the environment in which healthcare information is shared. It means systems are connecting routinely outside their organisational boundaries. While this currently exists to a certain extent, for example in primary care and sharing of laboratory results, it will ultimately evolve into a significantly more connected environment. This brings with it new security responsibilities, and highlights the need for increased awareness of the potential for security risks by managers, healthcare providers and others working in healthcare.

Taking established information security practices as a baseline, such as those provided by the National Institute of Standards and Technology (NIST 2005), the RACGP Computer and Information Security Standards (RACGP 2012), and the International Organization for Standardization (ISO 2008), a review of the new legislation in relation to Australia's e-health system and PCEHR was undertaken. Within this background, this paper does not take a blank canvas approach on security; it assumes that there are already security measures in place in the organisation. The paper provides an explanation of what has changed in regards to computer and information security in light of the PCEHR implementation and what is driving this change. A review of what should already be in place is also provided to give a point of reference for a subsequent discussion on what needs to be considered and addressed in regard to security in the new PCEHR security and e-health system. Further, the paper considers what other factors Health Information Managers (HIMs) should be aware of in the evolving e-health environment.

Drivers for change

In order to embrace the changes that need to be made to information security practices for the e-health environment, it is important to understand what underpins and is driving these changes. The requirement for secure electronic communication means both secure message transmission and secure use of the Internet. This is a result of the need for information transfer not only between healthcare providers and the PCEHR, but also between healthcare providers' organisations, patients and trusted third parties. Driving this are three key factors: expanded e-health functionality, compliance with legislation and directives, and new uses of technology.

Expanded e-health functionality

E-health provides new ways of doing business and supporting healthcare delivery. E-health encompasses timely and accurate transfer of information to support patient care, which includes the sharing of a patient's health summary with patient nominated parties. In addition, there are specific e-health initiatives such as the electronic transfer of prescriptions (ETP) between prescribers and dispensing entities. This expanded functionality will in some cases require improvement and alteration in healthcare processes using and generating health information. The new functionality and opportunity to practice healthcare utilising improved information sharing will result in a deeper understanding of what is possible. This potential and the realisation of these possibilities will drive change.

Compliance with legislation and directives

Obligations in regards to information privacy have existed for many years under the *Australian Privacy Act (1988)*, and this was expanded in 2012 by the *Privacy Amendment (Enhancing Privacy Protection) Act 2012,* which followed the Australian Law Reform Councils Report of 2008, and which

comes into force on 12 March 2014. There is now other new legislation specific to the Australian e-health system and PCEHR in place. These bring additional legal responsibilities to the Australian healthcare environment in the protection of information. This includes the following Commonwealth legislation and regulations, and directives from the Office of the Australian Information Commissioner (OAIC), and a framework from NEHTA[1]:

1. *Healthcare Identifier Act 2010* (incorporating amendments for the PCEHR Act 2012)
2. *Personally Controlled Electronic Health Records Act 2012* (PCEHR Act)
3. National Privacy Principles which will be replaced by the Australian Privacy Principles in March 2014
4. OAIC Data breach notification – a guide to handling personal information security breaches
5. OAIC Guide to information security: 'Reasonable' steps to protect personal information
6. NEHTA, National E-Health Security and Access Framework.

The implications of compliance with the legislation (numbered 1-3 above) in respect of additional security practices are discussed in detail in the 'new considerations in the Australian e-health context' section. The three directives listed (numbered 4-6 above) require more attention as these will drive good practice and governance process activities. These are the concepts of reasonable security protection, data breach notification, and the national e-health security framework.

The Privacy Act and National Privacy Principles stipulate that 'reasonable steps' are to be taken to protect and secure personal information, which includes health information. 'Reasonable steps' is further defined by the OAIC (Office of the Australian Information Commissioner 2012b). When investigating information security breach incidents and questions of compliance, the OAIC considers the steps that were taken to protect the information, and whether those steps were reasonable in the circumstances. This 'reasonableness' is considered in relation to the organisational context and the context in which the information is collected and used. Health information is defined as sensitive information in s.6 of the Privacy Act, and as such there is an expectation that such information will be given a higher level of protection than other types of non-sensitive information. This demands that both the protection and data breach processes are clearly articulated.

Data breaches occur through a variety of common situations, such as the loss or theft of laptops, mobile devices, removable storage devices, hard disk drives, and USB sticks. Breaches are not limited to electronic records and the security of paper records should also be considered; for instance theft from unsecured disposal is not infrequent. Less common, but harder to detect, is illegal access of databases from both outside the organisation through hacking, or from inside the organisation through access or disclosure by employees outside the bounds of their roles and authorisation. Unintentional breaches such as providing personal information to the wrong person, or sending it to the wrong address (physical or electronic) can and do already occur (Office of the Australian Information Commissioner 2012a). This includes situations where insufficient care is taken to confirm the identity of the person to whom information is disclosed. Australia now has mandatory data breach notification for the e-health record system as it pertains to the PCEHR under the *Personally Controlled Electronic Health Records Act 2012.* This is termed a 'notifiable' data breach. The legislation states that the System Operator, or Registered (PCEHR) Repository or Portal Operator must notify the OAIC. Individual healthcare providers and organisations do not have to report breaches to the OAIC because local systems are not covered by the PCEHR Act. However, under the PCEHR (Participation Agreement) Rules 2012, clause 4.4, they must notify the PCEHR System Operator (Australian Government ComLaw 2012d). Breaches of security that do not relate to the PCEHR system are out of scope of the mandatory data breach notification; however, the OAIC encourages voluntary data breach reporting in accordance with the Privacy Act (Office of the Australian Information Commissioner 2012a). More information can be obtained from OAIC website.

What is the national e-health security framework? A significant aspect of good security practice, which contributes to demonstrable information security governance, is the use of a framework to guide and support information security activities. Australia's e-health system security is underpinned by the National E-health Security and Access Framework (NESAF) (NEHTA 2012). The framework adopts a standard security risk assessment approach to security assessment by ensuring that management is aware of what is important, identifying what needs protection, assessing the risk to this information, selecting appropriate controls, and monitoring the results. This approach mirrors established best security practice in the industry, and together with treatment of data breaches must be accorded greater consideration in the new e-health environment.

New uses of technology

While not directly related to the e-health system and the PCEHR, the use of new technology is also driving change in security practice. The increased use and demand for mobile devices in healthcare, including what is termed BYOD (bring your own device) creates significant challenges in terms of security. However, use of such devices can contribute positively to the delivery of healthcare (Abernathy et al. 2008). So it too is a key factor in driving security change (Brand & Williams 2012).

Before addressing what needs to change, it is important to provide an insight into what security measures should already be in place.

Current practice

The basic premise for all information security practices is adoption and maintenance of the following:

- Confidentiality of information – only authorised people can access the information.
- Integrity of information – only authorised people can alter the information. Maintaining integrity includes the capture of quality data, preferably at the source when it is collected; periodic clinical review of information; the ability for the patient to review their own information; and control over versioning be available.
- Availability of information – it should be available and accessible when needed.

1 It is important to note that this reflects the co-regulatory nature of the Australian healthcare environment and that it is not just jurisdictional law that applies.

- Retention of data – this must be complete during the life of the patient and archived as based on the agreed criteria of the PCEHR Act for a period of 30 years following the death of a patient (up to 130 years where the date of death is unknown).
- Use of information for secondary use must be defined and managed for appropriate privacy and use.

Further, it is important to understand the difference between privacy and confidentiality. Privacy is concerned with the person, while confidentiality is about the information. Privacy relates to an individual's control over the use, disclosure and sharing of information that is collected about them. Confidentiality relates to the management of the information and the processes put in place to handle information once it has been disclosed. This includes how it is stored, the access control procedures, and how it is shared. Risk assessment processes, established security practice and fundamental measures are discussed briefly to provide a benchmark for what should already be in place and a baseline from which to discuss the changes required.

Risk assessment

All organisations should have a comprehensive understanding of the threats and vulnerabilities that they are open to, and the risk that these pose to the computer and information systems. Risk assessment includes articulating the legal and professional operating parameters of the organisation. This is essential to the understanding of what the compliance requirements for the organisation should be. Further, knowing who has access to which information systems is critical (e.g. by means of an audit log), as is recording details of all computer, information and software assets (more commonly known as an asset register). The biggest task is then to identify and rank the threats to, and vulnerabilities of, the assets that could adversely affect organisational operations. Subsequently, the levels of control must be matched to the vulnerabilities; the proposed controls to minimise the risk identified; and an action plan on how these will be implemented developed. The following standard security practices link to current practice and the accepted areas of risk existent in all health organisations. Risk assessment is a vitally important aspect of security and privacy to ensure that the controls in place are commensurate with the risks.

Standard security practice

Standard information security practices include the following aspects and should already be in place in the healthcare provider organisation.

Policy and procedures on roles and staff responsibilities. This information is used to define and administer access control to information systems. Policy should include all aspects of security listed below, and the procedures for how and when ongoing staff education is undertaken in respect to the various aspects and responsibilities regarding security. Even if a role is not responsible for setting policy, all staff should be aware of what the policies are, what an individual's responsibilities are and how to meet them.

Control and management of access. Access to systems should be consistent with the responsibilities outlined in the role description of each staff member. This includes the use of individual, strong passwords, removal of access when staff leave, and guidance on password management. With the plethora of information systems and associated logins, this is arguably the most complex task to manage in information security, particularly in large healthcare organisations.

Business continuity and disaster recovery plans. It is essential that all organisations have a business continuity plan in relation to their information systems. This management level activity is to support the critical functions in the event of a crisis. It enables continuation of essential functions without major disruption or risk to patients and staff. Additionally, the development and testing of a disaster recovery plan to return the organisation to its normal functioning state is required. Backup plays a critical part of the recovery process (as explained in more detail below). The business continuity plan uses the asset register (from the risk assessment process) to document the hardware and software and provides essential information such as where the computer media can be found, and who to phone for technical support.

Internet and email use. The Internet and email are common communication mediums and it is essential that the organisation has a policy that clearly states (and is communicated) the management and use of Internet and email by all staff. This will assist in mitigating security risks. In the age of social media such policy should also detail the organisational policy on access to social networking websites such as Facebook and Twitter.

Backup. Backup is a key component of business continuity and disaster recovery. Backup and recovery procedures should state that backup media are taken off site or are not accessible through the normal organisational network from outside. Where possible, backup processes should be automated, daily checking that the processes are working is necessary, and the data restoration process should be tested periodically.

Malware and virus protection. Malware and virus software installation, updating and monitoring procedures should be in place. It is essential that automated virus definition updates are done regularly (daily). Part of the mitigation strategy should include what to do if malware is detected.

Network perimeter controls. Network perimeter controls provide details of the systems (hardware and software) that protect the network. This may include firewall and intrusion detection and content filtering. These are by definition, technical solutions and require expert configuration and maintenance. These should be configured to reflect the business usage of the network and access to external networks, to ensure access and usability to external systems is balanced with adequate security measures.

Portable devices and wireless networks. The increasing demand for, and use of mobile devices, needs careful attention in the healthcare environment. Many organisations now make use of wireless networks, both for staff and patients, and it is essential that these are protected and access control to them strictly controlled. As an evolving area of innovation and adoption, mobile device use and remote access to information, for instance from home, needs specific consideration. Further discussion of this is as an emerging area of security concern is provided later in the paper.

Physical, system and software protection. The physical protection of hardware and systems should include restrictions on physical access to servers, securing equipment from theft, and damage by power interruptions. From a confidentiality perspective the use of screen savers and positioning of monitors to prevent unauthorised viewing of patient records and other confidential information is useful. Further, the safe

disposal of hardware and secure erasure of information on devices must be followed. Software and operating system maintenance is important and all software should be patched as soon as updates are available.

Secure electronic communication. Securing electronic information is important to prevent it being read by an unintended recipient. While phone calls can be tapped, faxes can go to the wrong person and letters can be opened by a range of people at a healthcare organisation or be delivered to the wrong address, electronic information transfer sets higher security standards. Electronic transmission makes it easier to inadvertently broadcast information to a wider audience yet offers the opportunity to protect information more efficiently than previous methods of transmission. The new e-health system and PCEHR is providing the infrastructure to support secure electronic communication. Encryption means that data is electronically 'scrambled' so that it cannot be read unless the information is decrypted. Authentication means that one can verify whether the sender is who they say they are, and this is done by using electronic signatures. E-health information exchange in the Australian health system relies on and incorporates encrypted, secure messaging techniques. The software programs used to handle this function are required to meet Australian standards.

New considerations in the Australian e-health context

With the increasing connection to information systems external to the healthcare entity, utilising the Internet and other networks, such as the PCEHR, it is essential that sound, basic security measures are in place, functioning correctly and processes being followed. These include access control, backups and malware protection as described above. In contrast, this section considers the impact of the new legislation and the implications of emerging technologies in the application to healthcare. Compliance with legislation is the biggest change associated with the PCEHR. It brings existing practices under the spotlight and requires more rigorous accountability in relation to information security management practices.

Impact of legislation

Driven by the new e-health environment and the PCEHR, new legislation has been enacted. Healthcare identifiers are a fundamental constituent in the secure transmission of data and patient identification. These are unique healthcare identifiers, comprising 16 digit identification numbers used to identify healthcare providers, healthcare organisations and individuals. Healthcare identifiers support the management of health information and the communication of health information between healthcare providers and organisations. The use and access of Healthcare Identifiers are governed by the *Healthcare Identifiers Act 2010.* Four types of healthcare identifiers are assigned by the Australian Healthcare Identifiers Service (HI Service):

- individual healthcare identifier (IHI) – for individuals receiving healthcare services
- healthcare provider identifier – individual (HPI-I) – for healthcare professionals and other health personnel involved in providing patient care
- healthcare provider identifier – organisation (HPI-O) – for organisations (e.g. a hospital or general practice) where healthcare is provided
- contracted service providers (CSP) – acting on behalf of a healthcare provider organisation.

Healthcare providers who are identified with an HPI-I, HPI-O or an authorised employee, can access the HI Service to obtain the IHI of a patient being treated. This means all staff will require training on the implications of healthcare identifier numbers and the protection of them, and the consequences of poor security behaviours. In addition, to participate in the Australian e-health system, healthcare organisations must use the secure message delivery services that support it. The certificates use Public Key Infrastructure (PKI) and are used for digital signing and for encryption functions.

The new legislation has particular requirements that need interpretation and application. For instance, the *Healthcare Identifier Act 2010,* s.5.27.a states that 'reasonable steps' to protect the personal information they hold from loss and from unauthorised access, use, modification or disclosure, or other misuse, are in place. Unfortunately, the stipulation of 'reasonable steps' to protect and secure personal information is the most loosely coupled aspect of the legislative compliance. However, it is closely linked to defensible governance and demonstrating best practice. Further, while all organisations must comply with the Privacy Act, to participate in the Australian personally controlled electronic health record (PCEHR) system organisations practices must also comply with the Healthcare Identifiers Act and the PCEHR Act and Rules. In addition, the Participation Agreement that all organisations must meet to engage in the PCEHR space, are derived from these legislations (Australian Government – ComLaw 2012d). Some of the major aspects of this that require attention include:

- Allocation of persons to the roles of Responsible Officer (PCEHR Rules) and Organisation Maintenance Officer (Health Identifiers Act) as the contact persons for the Health Identifiers Service and the PCEHR System Operator
- Notification of known and suspected data breaches that may affect the PCEHR to the System Operator
- Assuring that 'reasonable steps' to protect healthcare identifiers against misuse and loss, and from unauthorised access, modification or disclosure are in place as stipulated in the Health Identifiers Act (Division 5, 27 Protection of healthcare identifiers)
- Policy development and maintenance (Division 2 Security Requirements of the PCEHR Act and Rules) by:
  - Ensuring appropriate policy in regards to access control to the PCEHR, including how staff accessing the PCEHR will be trained and educated in security awareness; the process for identification of access requesters; the security measures in place; and the dissemination, enforcement, annual review and auditable version control of the PCEHR organisational policy.
  - Note the annual review must consider specific items to comply with the legislation and to encompass any relevant legal or regulatory changes that have occurred since the last review. These include the potential for the following events to occur:
    - unauthorised access to the PCEHR system using the healthcare provider organisation's information systems
    - misuse or unauthorised disclosure of information from a consumer's PCEHR by persons authorised

to access the PCEHR system via or on behalf of the healthcare provider organisation
- accidental disclosure of information contained in a consumer's PCEHR
- impact of any changes to the PCEHR system that may affect the healthcare provider organisation.

It must also be noted that PCEHR Rule 28 stipulates that those interacting with the PCEHR should not record document and record identifiers such as a patient's IHI, and the onus is on practices to ensure that staff are aware of this.

Data Breach notification is another major area of change, and arguably a more difficult one for organisations to meet effectively. Organisations are not legally required to report all data breaches except those that relate to the PCEHR. However, this is an area about which HIMs need to be informed and therefore able to promote awareness of it. The possibility of changes to the legislation to make data breach notification a more generally acceptable requirement should be considered. It is useful for organisational policy to document the procedures on the detection, action and reporting of breaches of security. This should incorporate identification of ongoing training needs of staff, reporting procedures and consequences for noncompliance with the policy. Instructions on what action should be taken if a data breach occurs or is suspected are also important. Specifically, under the conditions of the Participation Agreement to fulfil the requirements of the mandatory data breach notification that the System Operator and Repository and Portal Operators are bound to, practices must notify the System Operator if a breach or suspected breach has occurred in the circumstances where there is a non-clinical, PCEHR system-related error in a record that has been accessed via, or downloaded from, the PCEHR system; or the security of the PCEHR system has been compromised by you or one of your employees or by the use of your equipment (Australian Government – ComLaw 2012d). Reporting all incidents, both accidental and intentional, to meet the requirements of the PCEHR Act and any other (future) potential mandatory breach notification by the Office of the Information Commissioner should include details of the containment of the breach and mitigation strategies employed; the initial assessment of the cause of the breach; who should be notified; and details of the full investigation and recommendations. More specific content and appropriate recording from can be found in publications such as the RACGP Computer and Information Security Standards. It should be noted that future legislation may be brought in to make data breach reporting compulsory other than for the PCEHR, as occurs in other countries, and to be conformant with OECD guidelines.

New technologies

The impact of new technologies and the expanding application of existing technology need mention here because while not specific to e-health, the exposure to increased connectivity will encourage interest and demand to devices to increase productivity (Hughes 2012). From a security perspective it is not enough to consider computer and information security only for the fixed hardware. Remote access via wireless (Wi-Fi) connections and web-based access via Internet connections make it easier to log on to the information systems. In addition, the portability and small size of devices such as USBs mean that copying information is easier, whether for legitimate or unauthorised purposes. All portable devices should be password protected and encrypted where possible.

Remote access to the organisation's computer system includes wireless networks and increases the convenience of access to practice information. However, it also requires additional security measures so that eavesdroppers cannot gain unauthorised entry to your computer system. There is increasing use of Wi-Fi (or Bluetooth) enabled laptops and other handheld devices, for example for home and aged care visits, and you should obtain technical advice on how best to keep the equipment and information they hold secure. Wi-Fi devices must have encryption set up to ensure the confidentiality of information. Care should be taken when using devices in public places to avoid information being sighted, and connecting via open or unsecured public networks.

Further, remote access is also used by technical service providers to support computer systems. It must be ensured that the methods used to access your system for IT support cannot also become security vulnerabilities. Procedures should be in place to minimise these risks, such as by use of a Virtual Private Network (VPN). HIMs need to be mindful that third parties may have access to information systems legitimately and that contractual agreements for confidentiality should be in place. Additionally, it is important to review the security for staff home computers where practice staff take electronic files home to work on after hours and then return them to the clinic's network. Data needs to be secured (encrypted) on portable devices as they can be easily misplaced or stolen.

Organisation website safety and security

As organisations rapidly adopt Internet communications, an often-overlooked security vulnerability arises from the increasing use of websites for promoting healthcare provider services, and in particular appointment bookings. It is important that the information on organisation websites is up-to-date and does not invite unsafe practices. For example, patients might wish to contact the healthcare organisation via their website, but they need to be advised that sensitive clinical information should not be transferred in this way, and that there might be a delay in obtaining a response to their queries if they send a request in this way. The organisation must abide by the Guidelines for Advertising of Regulated Health Services set by the Medical Board of Australia (n.d.).

There might be additional security risks if the organisation website is hosted on the same computer that holds the organisational data. If there is a security breach through the organisation website there is a potential risk that the organisational data would be vulnerable. Your technical service provider will be able to advise on the best methods to secure your website as this may require the use of a demilitarised zone (DMZ) which separates the website and services that patients may access, from the main organisation systems.

Conclusions: implications for HIMs

HIMs should review and use good practice guides that are appropriate to their work environment. For instance, in primary care and office based practice a useful resource is the RACGP Computer and Information Security Standards and Templates. These include explanations of what needs to be done and why, together with Templates to support the

risk assessment process. It also provides a guide for practical improvement in security practices. The compliance with both the new legislation and OAIC governance requirements (in relation to protection of information and 'reasonable steps') means that using tools such as workflow Privacy Impact Assessments are also highly recommended. Additionally, the future use and impact of mobile health and BYOD needs consideration. This is not specific to the PCEHR, and is more about the evolution of computing in healthcare; however, it is something that needs to be proactively addressed.

Ultimately, whether or not information security is core to your role, individuals must become more aware of their responsibilities. If you are accountable for information security and the protection of health data, then adoption of good security processes are essential. Find a risk assessment resource and method that fits your particular workplace environment and work through it. While larger organisations, such as hospitals, may have an IT department that has overall responsibility for this, it is important that managers and staff understand their responsibilities within their specific work area.

The introduction of the PCEHR creates an altered perspective of what security is required. However, in reality if good practices are already in place then any additional measures are not onerous. What does become apparent is that everyone needs to be more cognisant of the issues that surround information security and their role in this. The advent of the new more connected, Australian e-health system, including the PCEHR, provides a good opportunity to review current security practices and identify areas for improvement. While it may not need a whole new paradigm for information security, it does require more focus on individual responsibility and compliance with regulation in a more overt manner. In a similar vein to the integration of occupational safety and health into work practices, whose responsibility is information security in your workplace? Well everyone's actually!

References

Abernethy, A.P., Herndon, J.E., Wheeler, J.L., Patwardhan, M., Shaw, H., Lyerly, H.K., et al. (2008). Improving health care efficiency and quality using tablet personal computers to collect research-quality, patient-reported data. *Health Services Research* 43(6): 1975-1991.

Australian Government – ComLaw (2012a). *Healthcare Identifiers Act 2010 incorporating amendments - C2012C00590*. Available at: http://www.comlaw.gov.au/Details/C2012C00590 (accessed 10 December 2012).

Australian Government – ComLaw (2012b). *Personally Controlled Electronic Health Records Act 2012 - C2012A00063*. Available at: http://www.comlaw.gov.au/Details/C2012A00063 (accessed 15 December 2012).

Australian Government- ComLaw (2012c). *Privacy Act 1988 - C2012C00414*. Available at: http://www.comlaw.gov.au/Details/C2012C00414 (accessed 6 January 2013).

Australian Government- ComLaw (2012d). *PCEHR (Participation Agreements) Rules 2012 - F2012L01704*. Available at: http://www.comlaw.gov.au/Details/F2012L01704 (accessed 2 February 2013).

Brand , M. and Williams, P.A.H. (2012). Mobile device management for personally controlled electronic health records: effective selection of evaluation criteria. In P.A.H. Williams & L. Coles-Kemp (Eds.) *Proceedings of the 1st Australian eHealth Informatics and Security Conference,* pp.28-24. Perth, ECISRI - Security Research Institute, Edith Cowan University.

Hughes, G. (2012). Mobile Device Security (Updated). *Journal of American Health Informatics Management Association* 83(4): 50-55.

ISO. (2008). *ISO 27799:2008 Health Informatics – Information security management in health using ISO/IEC 27002*. International Organization for Standardization.

Medical Board of Australia (n.d.). *Guidelines for advertising of regulated health services.* Available at: http://www.medicalboard.gov.au/Codes-Guidelines-Policies.aspx (accessed 24 April 2013).

NEHTA (2010). *NESAF Release 3.1: Standards Mapping (S1410)*. Available at: http://www.nehta.gov.au/connecting-australia/ehealth-information-security (accessed 21 November 2012).

NEHTA. (2011a). *Personally controlled electronic health records (PCEHR) program standards review: Recommendations on selection of standards v1.0.*Available at: http://www.nehta.gov.au/ehealth-implementation/pcehr-standards (accessed 21 November 2012).

NEHTA. (2011b). *Standards Analysis: PCEHR System v3.8*. Available at: http://www.nehta.gov.au/ehealth-implementation/pcehr-standards (accessed 21 November 2012).

NEHTA. (2012). *National E-Health Security and Access Framework v3.1*. Available at: http://www.nehta.gov.au/connecting-australia/ehealth-information-security (accessed 11 January 2013).

NEHTA. (2013). *PCEHR Standards.* Available at: http://www.nehta.gov.au/ehealth-implementation/pcehr-standards (accessed 12 January 2013).

NIST. (2005). *An introduction to computer security: the NIST Handbook (No. Special Publication 800-12):* National Institute of Standards and Technology.

Office of the Australian Information Commissioner. (2006). *National Privacy Principles*. Available at: http://www.privacy.gov.au/materials/types/infosheets/view/6583 (accessed 4 December 2012).

Office of the Australian Information Commissioner. (2012a). *Data breach notification – a guide to handling personal information security breaches.* Available at: http://www.oaic.gov.au/publications/guidelines/privacy_guidance/data_breach_notification_guide_april2012.html (accessed 4 December 2012).

Office of the Australian Information Commissioner. (2012b). *Guide to information security: 'Reasonable steps' to protect personal information (Consultation Draft December 2012)*. Available at: http://www.oaic.gov.au/news/consultations/Information_security/info_security_consult_draft_Dec2012.html (accessed 4 December 2012).

RACGP (2012). *Computer and information security standards and workbook.* Available at: http://www.racgp.org.au/your-practice/standards/ciss/ (accessed 1 December 2012).

Patricia A.H. Williams, *BSc(Hons), MSc, PhD*
eHealth Research Group Leader
School of Computer and Security Science
Edith Cowan University
270 Joondalup Drive
Joondalup, WA 6027
AUSTRALIA
Tel: +61 8 6034 5039
email: trish.williams@ecu.edu.au ■