Strengthening Legal Compliance for Privacy in Electronic Health Information Systems: A Review and Analysis

Vicky Liu, William Caelli, Lauren May

School of Software Engineering and Data Communications & Information Security Institute
Queensland University of Technology
GPO Box 2434 Brisbane Qld 4001, Australia

v.liu@qut.edu.au, w.caelli@qut.edu.au, l.may@qut.edu.au

Abstract

It is well recognised that adoption of information communication and technology (ICT) in healthcare can transform healthcare services. Numerous countries are seeking to establish national e-health development and implementation. To collect, store and process individual health information in an electronic system, healthcare providers need to comply with the appropriate security and privacy legislation. Deploying ICT systems in healthcare operations can provide advantages in healthcare delivery; however, risks to privacy in such e-health systems must be addressed. Adopting appropriate security technologies can simplify some of the complexity associated with privacy concerns.

Evaluation criteria can be useful in providing a benchmark for users to assess the degree of confidence they can place in health information systems for the storage and processing of sensitive health information. This paper provides an overview of the *"Common Criteria (CC)"* for the assessment of IT products and systems and relates privacy requirements to the relevant CC Protection Profiles. We recommend a certain level of security in healthcare related information systems. Healthcare providers need to deploy strong security platforms to ensure the protection of electronic health information from both internal and external threats including the provision of conformance in health information systems to regulatory and legal requirements.

Keywords

Security evaluation for health information systems, e-health and privacy, confidentiality, Electronic Health Records, Australian privacy legislation, HIPAA implications

1. Introduction

1.1 E-Health and Privacy

> *"... the problem of privacy in the end is nothing more and nothing less than the root problem of the relation of each one of us to our fellow men.*
> *What belongs to the citizen alone?*
> *What belongs to society?*
> *... timeless questions on the nature and place and destiny of man. "*[1]

In the 21st century information, computer and telecommunications technology and its artefacts (ICT) provide the critical infrastructure needed to support many essential services including requirements of the healthcare sector. The use of computer-based information systems and associated telecommunications infrastructure to process, transmit and store health information plays an increasingly significant role in the improvement of quality and productivity in healthcare. There is evidence [1] to demonstrate that the use of ICT in healthcare can reduce errors, improve patient safety and increase the quality of that healthcare service. Health records have clear requirements for managed confidentiality to safeguard personal privacy.

[1] Thomas J Watson, Jr; "Technology and Privacy", an address to the Commonwealth Club of California, April 15, 1968.

Proceedings of the National e-Health Privacy and Security Symposium 2006 (ehPASS'06) - ISBN: 1741071380 © 2006 QUT.

Privacy and confidentiality issues have plagued previous attempts at electronic health management systems. This paper advocates a fresh approach based on an IT architecture which is inherently more controllably secure than previous systems. The system proposed in this paper is based on a Mandatory Access Control (MAC) model.

E-health systems include a broad range of ICT applications that deliver healthcare services such as hospital management and information systems, electronic patient records, knowledge-based and expert systems, clinical decision making support systems, telemedicine, surgical simulations, computer-based assisted surgery and physician education. Electronic health records (EHR) are a fundamental building block of all e-health applications. Numerous countries, such as Australia, the UK, New Zealand and Canada, are all active in e-health initiatives. They are seeking to establish national e-health initiatives through requirements for the implementation of electronic health record systems coupled with the protection of privacy and confidentiality of such electronic health records.

In order to collect, store and process individual health information in an electronic system, healthcare providers, both public and private, need to comply with the appropriate security and privacy legislation and associated regulations. Thus, an understanding of both national and international legal requirements regarding the maintenance of electronic health records is necessary for the establishment of any framework for security management in health information systems (HIS). In the US, the *"Health Insurance Portability and Accountability Act (HIPAA)"* of 1996 has implications for major widespread reforms in the US healthcare sector. In the case of Australia, this means compliance with the Federal Privacy Act and jurisdictional State or Territory privacy and health record laws. It must be noted however that not all individuals have trust and confidence in the overall management of their health records or in the associated information systems used by healthcare providers. To instil an individual's trust and confidence, it is critical to ensure that sensitive electronic health information is maintained appropriately and that any such security measures are understood and accepted by an individual and by society at large.

To develop a reliable and secure HIS, we must ensure that appropriate levels of information security services and mechanisms are built into the HIS. This protects associated electronic health records against misuse, disclosure and unauthorised access, as well as providing guarantees of availability. Independent IT evaluation schemes can be beneficial in assessing the strength of security implementations in an HIS. Evaluation criteria can be useful in providing a benchmark for users to assess the degree of confidence that they can place in the HIS for the storage and processing of sensitive health information. Moreover, they provide a basis for specifying security requirements in the design, specification and purchase of an HIS. In turn, such IT evaluation criteria can provide guidance to system developers as to the type and level of security features required in their systems or products.

The proposed MAC-based system primarily satisfies the requirement for confidentiality of records. The healthcare management system application is then developed on this secured foundation. This approach is in stark contrast to current and previous healthcare management systems, which are based upon a Discretionary Access Control (DAC) model whose primary function is not confidentiality of information records. Information and communication technologies are sufficiently advanced that a MAC-based electronic healthcare management system is now quite feasible.

1.2 Paper Structure

This paper identifies and discusses issues relevant to the application of our proposed system and its healthcare management application. In conclusion, the paper describes a way forward for the development of the MAC-based healthcare management system.

Proceedings of the National e-Health Privacy and Security Symposium 2006 (ehPASS'06) - ISBN: 1741071380 © 2006 QUT.

Section 2 of this paper includes discussions of current e-health attempts and initiatives in the UK and Australia. It also addresses e-health concerns and considerations. Deploying ICT systems in healthcare operations can prove advantageous in healthcare delivery; however, risks to privacy in such e-health systems must be addressed.

Section 3 reviews the USA and Australian laws in regard to the protection of health information. The USA's HIPAA provisions may have widespread implications on the entire healthcare industry worldwide in addition to having an immediate affect on every information system that uses or processes health information in the USA.

Section 4 provides an overview of the *"Common Criteria (CC)"*, now international standard IS-15408, for the assessment of IT products and systems and relates privacy to relevant CC Protection Profiles.

Section 5 explains the basic concept of cryptography including exemplary applications using cryptographic techniques in e-health initiatives to ensure the security of electronic health records. Finally, some implications and conclusions are drawn in Section 6.

2. Current and previous e-Health Management Systems

2.1 E-Health Initiatives

In developing a new approach to the e-health management application, one needs to be aware of issues identified with current and previous attempts.

The current UK National Programme for IT (NPfIT) was initiated in 2002 as a ten-year project for providing electronic health record maintenance for 50 million patients[2]. Its goal is to connect 8,000 surgeries, 240 hospitals, 100,000 doctors and 380,000 by providing management of electronic health records, electronic booking of medical appointments and electronic prescribing. One of the program's criticisms is the perception of a lack of adequate security measures in place to protect the confidentiality of electronic patient records.

In Australia individual states and territories have their own individual programs. The current national e-health strategy is *"HealthConnect"*[3]which aims to implement a consistent national electronic health information system. Many aspects of *HealthConnect* have been criticised as well as the workability of the concept itself[4][5][6].

2.2. E-health Concerns and Considerations

ICT plays an increasingly significant role in the improvement of quality and productivity in healthcare. It is well recognised that adoption of ICT in healthcare is a critical enabler to transform healthcare services. Notwithstanding the obvious potential advantages of

---

[2] Brogan, B. "*Inquiry as NHS patient records go online*" from Telegraph Newspaper Online is available at http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2004/08/31/nhs31.xml, accessed 14/08/2006.

[3] *"What is happening – National"* is available at http://www.health.gov.au/internet/hconnect/publishing.nsf/Content/national-1lp, accessed 09/07/2006.

[4] More D., "*HealthConnect - A Major Rethink Required?"* is available at http://www.newmatilda.com/policytoolkit/policydetail.asp?PolicyID=106, accessed 16/07/2006.

[5] Howarth, B., "*Australia's e-records mess"* is available at http://www.govhealthit.com/article94797-06-12-06-Print accessed 15/07/2006.

[6] Braue, D., "*E-health gaining traction: Conference delegates*", is available at http://www.zdnet.com.au/news/software/soa/E_health_gaining_traction_Conference_delegates/0,2000061733,39205201,00.htm, accessed 17/08/2006.

Proceedings of the National e-Health Privacy and Security Symposium 2006 (ehPASS'06) - ISBN: 1741071380 © 2006 QUT.

deploying ICT in healthcare services, there are some concerns associated with integration and access to electronic health records. Information stored within electronic health systems is highly sensitive by its nature.

There is growing evidence worldwide that healthcare information systems are being rapidly connected to the Internet since most health information systems are designed and developed to be accessible through networked and distributed computing environments. Open usage of the global Internet's services, however, must be considered to be inherently insecure. This accentuates the public's concern for privacy.

A security violation in an HIS can cause catastrophic damage for healthcare providers and consumers in the case of unauthorised disclosure or alteration of individual health information. Goldschmidt [2] states that electronic health records may pose new threats for compromising sensitive personal health data. Moreover, Goldschmidt illustrates that malevolent motivations could disclose confidential personal health information on a more massive scale than possible with traditional paper-based medical records. Carter [3] states that successful implementation of electronic record systems must learn from the UK's previous health strategy experience. In addition, Quinne[7] discusses the fact that the largest threat to successful implementation of a national health information system is user adoption. User acceptability in e-health relies on the healthcare consumers' willingness to overcome the fear of privacy invasion in relation to their health information. There is also the factor of the healthcare service providers' willingness to adopt new technology that does not always facilitate working practices. To convince healthcare service consumers and providers to use electronic health records, it is crucial to instil confidence that electronic health information is well protected and that privacy is assured.

Adopting appropriate security technologies can help address some of the complexity associated with privacy concerns. Moreover, security technologies such as computer and data network access control mechanisms and cryptography can ensure the security of electronic health records.

It may be argued that the maintenance of suitable levels of security in electronic health systems can be effectively monitored and enforced by legislation and regulation. Thus, an understanding of international/national legal requirements and standards regarding the maintenance of electronic health records could be seen as necessary for the establishment of any framework for appropriate security management in an HIS.

3. An Overview of Privacy Laws and Legislations Related to Health Information Protection

'Privacy' is concerned with the rights of an individual. This is in contrast to the rights of society as a whole or the rights of an organisation or state. In these broader applications we generally discuss confidentiality issues with the more generic terminology 'security'. Ensuring individuals' privacy is a major concern of an e-health management system. To ensure citizens' privacy is protected, governments legislate 'privacy principles'.

This section provides an overview of the current regulatory environments in the USA and Australia, including the Australian Federal Government, the States and Territories. Section 3.1 emphasises the key concepts of the USA's HIPAA Security and Privacy Rules which contain security requirements relevant to implementation of the security controls in any HIS. Section 3.2 outlines the Australian Federal Privacy Act and relevant Australian State/Territory privacy laws and health record legislation.

[7] Quinn, J., "*Lessons from the UK EMR: Not Exactly Apples to Apples*" is available at http://www.healthleaders.com/news/print.php?contentid=60316, accessed 17/08/2005

Proceedings of the National e-Health Privacy and Security Symposium 2006 (ehPASS'06) - ISBN: 1741071380 © 2006 QUT.

3.1 USA Privacy Laws and Health-related Privacy Legislation

3.1.1 HIPAA Overview

HIPAA [4] was enacted in 1996 by the USA's Congress. The USA's Secretary of the Department of Health and Human Services (HHS) is mandated with the responsibility and authority to implement and enforce HIPAA. HIPAA is a broad Federal statute that addresses numerous healthcare related topics. *Under "Subtitle F - Administrative Simplification of Title II of HIPAA"* three types of entities, referred to as *"covered entities",* are affected: healthcare providers, health plans, and healthcare clearinghouses. The purpose of HIPAA provisions is to encourage electronic transactions and to require safeguards to protect the security and confidentiality of health information.

HIPAA Administrative Simplification consists of four sub-sections: Privacy Rule, Security Rule, Electronic Transactions and Code Set, and Unique Identifier Rules.

The Office for Civil Rights (OCR) implements and enforces the Privacy Rule. The Centre for Medicare and Medicaid Services (CMS) undertakes administration and enforcement of all other Administrative Simplification activities including the Security Rules. Covered entities are required to analyse the nature and resources of their businesses to determine reasonable and appropriate measures to ensure the security of *"protected health information (PHI)"* [5].

3.1.2 Security Rule

The primary goal of the Security Rule is to protect the confidentiality, integrity and availability of "*individually identifiable health information (IIHI)",* i.e. protected health information (PHI). The Security Rule is relevant to all "*electronic protected health information (EPHI)"* the covered entity creates, receives, maintains or transmits. Most covered entities were to be in compliance with the Security Rule no later than 20 April 2005, with compliance for small health plans to be no later than 20 April 2006 [6]. The security standards defined in the Security Final Rule are intended to be technology-neutral. Covered entities have options in selecting the appropriate technology to protect EPHI, based on the nature and resources of their business [5].

The implementation specifications of the Rule are separated into two types: "required" and "addressable". A covered entity can make implementation decisions on addressable implementation specifications but must meet the required implementation specifications. The Security Final Rule consists of three categories of security safeguards including: administrative, technical and physical safeguards. In particular, the technical safeguards include the security technology and related policies and procedures that protect EPHI, including access control, audit, integrity, person or entity authentication and transmission security [5] .

3.1.3 Privacy Rule

The Privacy Final Rule protects all forms of PHI maintained or transmitted by a covered entity or its business associate. There are no restrictions on the use or disclosure of de-identified health information. The Privacy Final Rule grants individuals new rights which will permit them to access their health information and allow them to control how it is used. Generally, PHI can be used or disclosed by covered entities for the purposes of treatment, payment and healthcare operations. The Privacy Final Rule requires covered entities to implement appropriate administrative, technical, and physical safeguards to protect PHI from any intentional or unintentional use or disclosure that violates the Rule [5].

The Privacy Rule defines situations or purposes on the permitted uses and disclosures of PHI. There are also civil, monetary and criminal penalties for failure to comply with the

Proceedings of the National e-Health Privacy and Security Symposium 2006 (ehPASS'06) - ISBN: 1741071380 © 2006 QUT.

Privacy Rule. For most covered entities, compliance requirement with the Privacy Rule was required as of 14 April 2003, with compliance by small health plans to be by April 2004 [6] .

The "Minimum Necessary" standard is a key provision in the Privacy Rule. To prevent unnecessary or inappropriate access to and disclosure of PHI, a covered entity must make reasonable efforts to limit the use or disclosure of, and requests for, PHI to the minimum necessary to accomplish the intended purpose. Covered entities must develop and implement minimum necessary policies and procedures that control access and uses of PHI based on the job functions and the nature of the business. These minimum necessary policies and procedures must identify the persons or classes of persons within the workforce who need access to PHI, the categories of PHI needed, and circumstances appropriate to such access, to achieve necessary tasks [5].

3.1.4 Security Rule and Privacy Rule – "No security, no privacy"

Beaver and Herold [7] state that security is the strategy and privacy is the consequence. Security has long been recognised as having three major aspects, including confidentiality in addition to integrity and availability. The requirements of the Privacy Final Rule may overlap with some requirements of the Security Final Rule. For instance, the Privacy Final Rule requires covered entities to adopt appropriate administrative, physical and technical safeguards and to implement those safeguards reasonable for the protection of the privacy of a PHI. Compliance with these requirements of the Privacy Final Rule will also satisfy the requirements of the Security Final Rule [5].

While security and privacy are very closely related, they can involve distinct activities. It is important to note major differences between the Privacy and Security Final Rules. The Security Final Rule covers PHI in electronic form only; nevertheless, the Privacy Rule applies to all forms of PHI including oral, written or electronic form. The Security Rule defines administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of EPHI. The Privacy Final Rule, by contrast, asserts that a covered entity must implement appropriate administrative, technical and physical safeguards to protect the privacy of PHI from intentional or unintentional use or disclosure that is in violation of the standards. Additionally, the Privacy Final Rule defines the criteria on the use or disclosure of PHI and individuals are granted new rights to access their health information [5].

3.1.5 HIPAA Implications

HIPAA will have a tremendous impact on existing technology, as well as requiring the consideration of new technology to effectively support a comprehensive, compliant strategy. ICT products and systems enable an effective safeguard strategy to assist the healthcare industry to comply with HIPAA requirements. HIPAA covered entities need to clearly identify the specific standards and implementation specifications that map their policies and procedures to conform to HIPAA requirements.

HIPAA prescribes no particular software or technology to protect PHI. The HIPAA Security Final Rule generalises the access control standards from the previous proposed regulations. No specific access control mechanisms are identified. Any appropriate access control method is allowed. It is worthwhile to note that there are several definitions in the proposed regulations that are removed from the definitions in the Final Rule, such as role-based access control and usage-based access control. It has been apparently considered too restrictive to just include specific kinds of access control mechanisms. There are a variety of access control methods available, such as mandatory access control (MAC), discretionary access control (DAC), time-of-day parameters, object classification, subject-object separation and partitioned rule-based access control.

Proceedings of the National e-Health Privacy and Security Symposium 2006 (ehPASS'06) - ISBN: 1741071380 © 2006 QUT.

There are numerous security enhancing techniques available, such as digital signature or checksum technologies, that ensures that the integrity of EPHI in covered entities' possession is maintained and that records have not been altered or destroyed in an unauthorised manner. Likewise, there are a number of techniques that can be used to authenticate users, such as biometric identification, password systems, personal identification numbers (PIN) and even well-understood telephone callback[8] systems.

Use of encryption technology for transmitting EPHI is an addressable implementation specification. The Security Final Rule does not specify any encryption strength, since technology evolves so rapidly. Network-technologies such as Virtual Private Networks (VPN[9]), Network Layer Security (IPSec[10]) and Secure Sockets Layer (SSL[11])/Transport Layer Security (TLS[12]) may be used as possible solutions to address the transmission security of EPHI. In any event, the Security Rule allows covered entities to adopt reasonable and appropriate technical safeguards to protect EPHI based on their circumstances [8].

3.2 Australian Privacy Laws and Health-related Privacy Legislation

Australian privacy legislation encompasses several statutes including Federal, State and Territory laws.

3.2.1 Australian Federal Government

The principal Federal statute is the Privacy Act 1988 [9] which has provisions for the protection of the privacy of personal information including eleven *"Information Privacy Principles (IPPs)".* The Commonwealth and ACT government agencies are subject to these eleven IPPs. They address how federal and ACT government agencies should collect, use and disclose as well as provide access to personal information including the ability to grant individuals certain rights to access their personal information and correct errors [10].

The Privacy Amendment (Private Sector) Act 2000 was enacted to extend the application of the Privacy Act 1988 to cover the protection of personal information held by private sector organisations throughout Australia. These amendments to the Privacy Act 1988 (Commonwealth) contain ten *"National Privacy Principles (NPPs)".* The NPPs apply to large private sector organisations with an annual turnover of more than $3 million (Aust) and all health service providers in the private sector. The NPPs stipulate how private sector organisations should collect, use and disclose, keep secure, and provide access to personal information [11].

Undue emphasis on and control of confidentiality, however, could make access to personal health data difficult for medical studies, which could put the integrity of medical research at risk. Guidelines s.95 [12] and s.95A [13] balance the protection of the confidentiality of individual health information with the need for ethically approved research using such individual health data without consent from the individual(s) involved. The Guidelines

---

[8] A security feature used to authenticate users calling in to a network. During callback, the system authenticates the caller's identity, hangs up, and then returns the call, either to a number requested during the initial call or to a predetermined number. http://www.microsoft.com/technet/prodtechnol/visio/visio2002/plan/glossary.mspx accessed 22/11/2005.

[9] A VPN is a network scheme connected via Internet, but information sent across the Internet with encryption and other security mechanisms to ensure that only authorised users can access the network and the transmitted data cannot be intercepted by unauthorised party. http://webopedia.internet.com/TERM/V/VPN.html accessed 22/11/2005.

[10] IPSec is a security mechanism for ensuring secure communications over open networks through the use of cryptographic security services. IPSec supports network-level peer authentication, data integrity and data confidentiality http://www.microsoft.com/windowsserver2003/technologies/networking/ipsec/default.mspx accessed 22/11/2005.

[11] SSL, designed by Netscape, is a commonly used protocol for endpoint authentication and communications privacy using cryptography on the Internet. http://en.wikipedia.org/wiki/Secure_Sockets_Layer accessed 18/06/2006.

[12] TLS, designed by IETF, is a non-proprietary protocol. It is derived from SSL and has almost identical to SSLv3 http://en.wikipedia.org/wiki/Transport_Layer_Security accessed 18/06/2006.

Proceedings of the National e-Health Privacy and Security Symposium 2006 (ehPASS'06) - ISBN: 1741071380 © 2006 QUT.

provide guidance for the conduct of research relevant to public health or public safety and for human research ethics committees to follow when considering proposals. Guideline s95 applies to medical research that involves access to personal information held by Commonwealth agencies where identified information needs to be used without consent from the individual(s) involved. Guideline s95A applies to medical research that involves access to personal information held by organisation in the private sector.

3.2.2 Commonwealth/Federal – State and Territory Privacy Acts

Table 1 indicates the general structure of the privacy legislation in Australia.

Table 1 General structure of privacy legislation in Australia

Jurisdiction	Law-Regulation-Code-Standard	Covered Entity	Effective Date	Relevant Guidelines
Cth	Privacy Act 1988	Commonwealth and ACT government agencies	1988	Guidelines to the Information Privacy Principles http://www.privacy.gov.au/act/guidelines/index.html
	The Privacy Amendment (Private Sector) Act 2000	Some private sector organisations	21-12-2001	Guidelines to the National Privacy Principles http://www.privacy.gov.au/publications/nppgl_01.html
ACT	Australian Capital Territory Government Service (Consequential Provisions) ACT 1994	Public sector		
	The Health Records (Privacy and Access) Act 1997	Public and private sectors	01-02- 1998	
NSW	Privacy and Personal Information Protection Act 1988 (PPIP)	Public sector agencies		
	Health Records and Information Privacy Act 2002 (HRIP)	Public and private sectors	01-09-2004	4 statutory guidelines under the HRIP Act. http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/pages/PNSW_03_hripact#4b
VIC	Victorian Information Privacy Act 2000	Public sector	01-09-2002	
	Health Records Act 2001	Public and private sectors	07-01-2002	
	Health Records Regulations 2002	Public and private sectors	07-01-2002	
QLD	**No privacy laws** Information Standard No 42 - Information Privacy (IS42)	Public sector	Sep-2001	IS42 Information Privacy Guidelines http://www.governmentict.qld.gov.au/02_infostand/downloads/is42guidelines.pdf
	IS Information Privacy for the Queensland Department of Health (IS42A)	Queensland Health	Sep-2001	IS42A Information Privacy Guidelines http://www.governmentict.qld.gov.au/02_infostand/downloads/is42aguidelines.pdf
SA	**No privacy laws** Cabinet Administrative Instruction 1/89	Public sector	Jul-1992	
	Code of Fair Information Practice	Public sector, including the Department of Health and/or funded service providers	Jul-2004	
WA	**No privacy laws**. a public discussion paper released on 20 May 2003			
TAS	The Personal Information and Protection Act 2004	Public sector including the University of Tasmania	5-09-2005	
NT	Northern Territory of Australia Information Act 2002	Public sector	1-07-2003	
	Northern Territory of Australia Information Regulations	Public sector	1-07-2003	
	No specific health information protection laws.			
ACT	Privacy Act 1988	Commonwealth and ACT government agencies	1988	Guidelines to the Information Privacy Principles http://www.privacy.gov.au/act/guidelines/index.html
	The Health Records (Privacy and Access) Act 1997	Public and private sectors	1-02-1998	

3.2.3 The Need for a Nationally Consistent Health Regime

To date, Australia has not established a nationally consistent approach to handle health information legislation, like the USA's HIPAA. The National Health and Medical Research Council[13] (NHMRC) describes health information as a particular subset of personal information, so that health privacy is set within the general privacy framework. The relevant privacy legislation in Australia includes the Commonwealth Privacy Act . As indicated in Table 1, some States and Territories have their own privacy legislation, health record Acts, information standards, codes of conduct, guidelines and the use of common law for the protection of health information. In fact, the Commonwealth, Victoria, NSW, ACT, Tasmania and the Northern Territory have various forms of privacy legislation. There are no specifically independent laws to address the privacy of health information in QLD, SA and

[13] "Health Privacy Framework" is available at http://www.nhmrc.gov.au/ethics/human/issues/privacy.htm#1, accessed 20/06/2006.

Proceedings of the National e-Health Privacy and Security Symposium 2006 (ehPASS'06) - ISBN: 1741071380 © 2006 QUT.

WA, but these states have administrative standards and obligations. Fernando [14] raises the concern that the problems of overlap in federal, state and territory privacy laws create complexity and confusion in the health privacy legislative environment. It is a challenge to develop HISs that are compliant with a complex patchwork of health privacy laws. This could also impose upon an organisation high costs or impediments in attempting to conform to either the relevant jurisdictional or federal privacy laws. Undoubtedly, the need for establishing a nationally consistent privacy regime to adequately protect the security of health information is paramount.

Recently, the Australian Government developed a draft for a National Health Privacy Code [15]. There are eleven National Health Privacy Principles (NHPPs) within the Code. The goals of the Code are to protect health privacy and to achieve national consistency in health privacy protection across jurisdictions and between the public and private sectors. The proposed Code considers the way individual health information is managed as a result of technological change. The Code also contains some new components intended to facilitate the secure exchange of health information between jurisdictions and across electronic health information networks.

4. Security Evaluation for Health Information Systems

In order to realise success with any ICT system design where security features are important it is essential to be able to demonstrate that the system achieves its stated security objectives. This can be realised through the application of a Security Evaluation Scheme. In e-health initiatives, special safeguards need to be established to ensure that the information collected, disclosed and shared through any HIS is kept confidential and is protected from misuse and unauthorised access, accidental or deliberate, from both internal and external sources. Given the increased sophistication of ICT technology, there is an acknowledged need for international standards to be used to evaluate the security level of any HIS.

4.1 ICT Security Evaluation Schemes

Over the last 25 years, there have been a number of internationally recognised and accepted evaluation schemes that may be used to assess the strength of security architecture and implementation in ICT products and systems in general, including health-related systems. Some of these are the USA's Trusted Computer Security Evaluation Criteria (TCSEC) [16] (often cited as the "Orange Book" with associated documents known as the "Rainbow Series"), the European Information Technology Security Evaluation Criteria (ITSEC) [17], and the Canadian Trusted Computer Product Evaluation Criteria[14] (CTCPEC).

These evaluation criteria, along with others, have been largely superseded by the internationally accepted *"Common Criteria (CC)"* for such evaluation [18]. The CC is an international standard for developing security specifications and performing security evaluations of resulting products and systems, with the main goal being to harmonise and align the earlier TCSEC, CTCPEC and ITSEC above, as well as other national initiatives in the area. It was designed and developed through multinational efforts.

The CC provides a common set of security requirements for IT products or systems under the distinct areas of functional requirements, and assurance/evaluation requirements. The functional requirements define desired security behaviour. Assurance or evaluation requirements are used as the bases for gaining confidence that the claimed security measures are effective, reliable and robust and are implemented correctly.

4.2 Essential Concepts of the CC

[14] CTCPEC is available at http://en.wikipedia.org/wiki/CTCPEC, accessed 02/08/2006.

Proceedings of the National e-Health Privacy and Security Symposium 2006 (ehPASS'06) - ISBN: 1741071380 © 2006 QUT.

There are a number of basic concepts and terms in the CC that need to be defined. These are:

- Target of Evaluation (TOE): the part of an ICT product, application or system being evaluated, including its documentation, that provides the functionality to counter the threats defined in its "Security Target".
- Security Target (ST): the security functionality and assurance measures required in a product or system along with the environment in which they are designed to work.
- Protection Profiles (PP): a set of security functionality and assurance requirements, often with a specified EAL, for an ICT product or system that meets some particular need. It normally contains an outline of a set of relevant threats with security function requirements and assurance activities along with a justification of how these address the threats [19].

Essentially a (TOE,ST) pair is assessed for compliance with a PP. The assessment is performed with respect to CC evaluation levels.

4.2.1 Evaluation Levels

Evaluation is a check of processes employed. The evaluation assurance levels in the CC range from "EAL1", the lowest, to "EAL7", the highest. Each assurance level places increasing demands on the developer for evidence and testing [19].

Evaluation performed up to the EAL4 level requires the examination of design documents, management procedures and allied factors in the creation of products, using non-challenging criteria. Evaluations from EAL5 to EAL7 require software code examination, for example, along with even more formal definition of security relevant structures by the security system architects and developers. In particular, EAL7, the highest rating, requires that key parts of the ICT product or system be rigorously verified in a mathematical way [20].

4.3 Protection Profiles

A range of PPs is being developed addressing security needs for access control devices and systems, operating systems, databases, network boundary protection devices and systems, smart cards related devices and systems and other application needs. In relation to the privacy of healthcare systems an examination of relevant operating system, access control related PPs is needed. This includes:,

- Controlled Access PP,
- Labelled Security PP,
- Role Based Access Control PP, and
- Healthcare systems related PPs.

4.3.1 Controlled Access Protection Profile (CAPP)

Firstly, the assurance level of the CAPP [21] is "EAL 3", a rather low level. The CAPP adopts the earlier *"Discretionary Access Control (DAC)"* policy of the 19893 TCSEC to enforce access limitations on individual users and data objects. DAC allows system users to decide on the type of access to be given to other users at the discretion of the owner of the information. Such a policy does not provide capability to the actual owner of the system to define and enforce a fully centralised access control policy over an enterprise's information resources. CAPP compliant products should also provide an audit function to record any security relevant events that may occur within the system. The CAPP is designed to protect assets in a "moderate" risk environment. It is vital to note that under this protection profile the level of protection requirement is based on the assumption that products or systems operate in a non-hostile, benign and cooperative community. Such an environment clearly does not apply to computer systems connected to the global Internet whereby, for example, programs from sources outside the DAC environment may be introduced into the system

4.3.2 Labelled Security Protection Profile (LSPP)

Proceedings of the National e-Health Privacy and Security Symposium 2006 (ehPASS'06) - ISBN: 1741071380 © 2006 QUT.

The assurance level of the LSPP [22] is "EAL 3 augmented". LSPP conformant products should support two classes of access control mechanism, namely DAC, as above, and *"Mandatory Access Control (MAC)"*. With the MAC policy, the overriding information access rule is based on a concept of "clearances" for users and "classification" for information defined by the owner of the information system and not by its users or developers. Access permissions are determined by a user's clearance compared with the sensitivity or classification level label on information stored in the system, not upon the user's discretion. The LSPP is designed to protect assets in a moderate risk environment. This protection profile provides for a level of protection under the assumption that products may not operate in the non-hostile and benign community.

4.3.3 Role-Based Access Control Protection Profile (RBAC PP)

The assurance level of the RBAC PP [23] is a very low "EAL 2". The RBAC PP specifies security functionality and assurance requirements for general purpose operating systems, database management systems, systems management tools and other applications. RBAC compliant TOEs should support user's access rights based on such parameters as job function, enforcement of least privilege for administrators and users, enforcement of separation of duties, and hierarchical definitions of roles. The objective of RBAC is to simplify and streamline the management of user authorisation to reduce the probability of mistakes and thereby strengthen assurance of a system's overall security.

4.3.4 Health Related Protection Profiles

Indeed a PP for the privacy and security of both electronic health and medical records would be a valuable addition to the library of the protection profiles available under the *"Common Criteria Recognition Arrangement (CCRA)".* Such a health protection profile initiative[15] has been under development since 1999 but, unfortunately, no published protection profile for healthcare has eventuated. However, in relation to appropriate sub-systems, PPs related to health "smart cards" have been published: Protection Profile for electronic Health Card (PP eHC) [24], and Protection Profile for Health Professional Card (PP HPC) [25]. These PPs have set an evaluation level of "EAL4+". They specify sets of security features for eHC and electronic HPC respectively according to the regulations of the German healthcare system. They specify appropriate authentication parameters for cardholders along with levels of security for stored data, etc.

4.4 Privacy Requirements and CC PPs

The USA's *"HIPAA Final Rule"* does not prescribe any particular access control mechanisms or any particular technology to protect PHI, apparently in order to embrace the principle of "technology neutrality". Any appropriate access control method can be used to protect PHI. In Australia, relevant privacy legislation, including jurisdictional health record laws, addresses the privacy requirements for the protection of personal information via a broad approach. An entity is required to implement reasonable steps to safeguard personal information it holds from unauthorised access, modification or disclosure.

In general, current regulatory requirements for privacy in healthcare systems do not restrictively impose the use of any specific computer software or allied technology for data protection since they are intended to be technology-neutral. These requirements are also meant to provide minimum guidelines to healthcare providers. It is easily argued that it is worthwhile for healthcare providers to consider providing a tailored product that better meets the needs of the healthcare industry than that specified as the minimum requirements set. From a business viewpoint a superior product has many advantages: desirability in the marketplace, long-term potential, continual enhancement opportunities, a relatively captive market, etc. The technical processes and procedures which would enable a higher standard

[15] NIST, "*Health Care Protection Profile Initiative"* is available at http://csrc.nist.gov/nissc/1999/proceeding/papers/o19.pdf accessed 05/08/2006.

Proceedings of the National e-Health Privacy and Security Symposium 2006 (ehPASS'06) - ISBN: 1741071380 © 2006 QUT.

of healthcare product are available today. It is entirely feasible to develop current technology into a practical workable solution for the healthcare industry at a standard exceeding the current minimum requirements. The end-product would protect health records by providing stricter access control measures, thereby preventing unauthorised access.

Our approach to addressing this issue is to develop Mandatory Access Control (MAC) techniques to a sufficiently high, yet useable, standard that would enable an effective operational-level foundation on which to further the design and development of health applications. Currently, the generic CAPP, by adopting a Discretionary Access Control (DAC) policy, allows "owners" of data (typically end users) to enable access to that data in a completely arbitrary manner. Under DAC the "owner" of the system is dictated by its end users with respect to access to enterprise data. DAC policies, therefore, encourage weak access control requirements that effectively provide inadequate protection against penetration by such "malware" as "viruses", "trojans", "spyware", "rootkits" and other malicious program code. As a consequence it may be readily asserted that a product or system only meeting CAPP requirements does not enable sufficient security protection for Internet and allied connected health-related systems.

With MAC, the delegation of access permissions is taken out of the hands of system users and software developers. In effect, MAC policy enables the system to define and enforce an overall, enterprise-defined set of data access and program activation rules. Typically these rules are based upon the requirements of the system application and associated legal parameters and/or regulations. Thus, in the case of healthcare information systems such rules would be developed to satisfy health regulation requirements. Appropriately, the CC's LSPP embraces both the DAC and MAC policy rules and sets strict access limitation on both users and data objects. In addition, a product or system meeting the LSPP provides better resistance to unauthorised access to the system.

Another important concept, currently available through modern MAC systems, is Role-Based Access Control (RBAC), defining an individual's role in the organisation as a major parameter rather than just a user's individual identity. The driving force behind the RBAC policy is thus to simplify and make more flexible the management of authorisation.

5. Protection and Enforcement Using Cryptography

Cryptographic technologies have long been used for integrity and confidentiality purposes. (It is important to understand that the principle role of cryptography is to ensure the quality of service of the technology, and thus ensure that the technology satisfies the business requirements of the system. Cryptography, then, is primarily an enabler of services; detection and prevention of security breaches is a subset of this primary function.) For integrity, a *"keyed hash function"* may be applied to each relevant data record to prevent unauthorised insertion of records as well as unauthorised alteration of existing records. An unauthorised third party (or an authorised party extending beyond their authorisation) would need to possess the necessary key to either create or re-make the integrity enforcing checksum, commonly referred as a *"message authentication code (MAC)".* Confidentiality can be enforced using a single-key cipher, but key management structures to allow for multiple roles to have access to a healthcare record would be necessarily complex. As such, maintaining record confidentiality using public key cipher schemes may be advantageous. Historically with this approach, a performance penalty may have been involved, but with current hardware bases for the implementation of these ciphers, such performance problems are normally minimal.

Encryption should be used, and normally is used, to protect data in transit for complete end-to-end protection; where the term 'end-to-end' refers to the two end nodes themselves as

Proceedings of the National e-Health Privacy and Security Symposium 2006 (ehPASS'06) - ISBN: 1741071380 © 2006 QUT.

well as the communication link between them. Data in storage should also be encrypted for end-point security against unauthorised or accidental access or eavesdropping.

For end-to-end security, UK NHS is undertaking *the "Cryptography and the Pathology Messaging Enabling Project*[16]*"* for the implementation of national standard pathology messaging. For such a large-scale project, the NHS has adopted a "Public Key Infrastructure (PKI)" scheme to provide transmission security for pathology messages through data encryption and digital signature technologies. The New Zealand Health Information Service uses the *"National Health Index*[17] *(NHI)"* numbering scheme to uniquely identify individuals for treatment and healthcare purposes. Within the NHI numbering system, each individual record contains a unique NHI number associated with personal information. The NHI numbering system is linked to a separate clinical information system, the *"Medical Warnings System (MWS)"*. The MWS can only be accessed through the associated NHI number. All NHI messages are protected by an encryption technique while they travel over the Health Intranet via VPN technology. The encrypted form of the NHI number is used for clinical or analytic studies, rather than removing all personally identifiable information. This would make data anonymous to protect the privacy of individuals.

At the commercial level, RSA Security Inc. of the USA has launched a software system using database encryption, in conjunction with digital signatures, to protect patient information. However, encryption of "data at rest", i.e. data contained in database systems on disk storage and on various "backup" storage media, still does not seem to be widespread and a literature analysis has failed to indicate any major trend in this area.

6. Some Implications and Conclusions

ICT is now sufficiently advanced that a MAC-based electronic healthcare management system is feasible. This approach would overcome many of the privacy and confidentiality issues which have plagued previous attempts at electronic health management systems. The Mandatory Access Control operating system primarily satisfies the requirement for confidentiality of records, which has shown to been a major impediment to current and previous systems. The healthcare management system is then developed atop the secure MAC-based operating system.

This paper has reviewed current ICT security architectures and standards. It is suggested that the healthcare community should adopt a policy of purchase and operation of overall information systems that are certified at a CC "EAL4" level, at least, when such information systems contain personal health data. The PP should be at least based around the LSPP definition enabling overall enterprise security and privacy rules to be defined and enforced. At the present, there appears to be no "EAL6" level, general purpose operating system commercially available "off-the-shelf" [26]. It could also be recommended that any application or sub-system responsible for the security enforcement activities for individually identifiable health information must be evaluated at least at a level of "EAL5", and preferably higher. This would include, in particular, any appropriate cryptographic sub-systems for such usage. Commercial computer and network systems currently, or soon will, exist to meet these requirements. Examples include:

- "Red Hat Enterprise Linux (RHEL) Version 4 Update 1 AS",
- "Red Hat Enterprise Linux (RHEL) Version 4 Update 1 WS",
- "Trusted Solaris 8", and others.

Undoubtedly, health information is highly sensitive by its nature. Therefore, it is critical to protect such information from any security hazards and privacy threats. It is argued that

[16] "*Cryptography and the Pathology Messaging Enabling Project*" is available at http://www.connectingforhealth.nhs.uk/pathology/security_and_encryption/crypto_v5/, accessed 15/08/2006.

[17] "*National Health Index*" is available at http://www.nzhis.govt.nz/nhi/index.html, accessed 15/08/2006.

Proceedings of the National e-Health Privacy and Security Symposium 2006 (ehPASS'06) - ISBN: 1741071380 © 2006 QUT.

adoption of appropriate security technologies, including in particular MAC oriented operating system bases for such systems, can help demystify some of the complexity associated with the maintenance of confidentiality of healthcare records.

Figure 1 illustrates a general architecture for a modern healthcare information system, which consists of health application services, middleware, database management system, network control system, operating system and hardware.

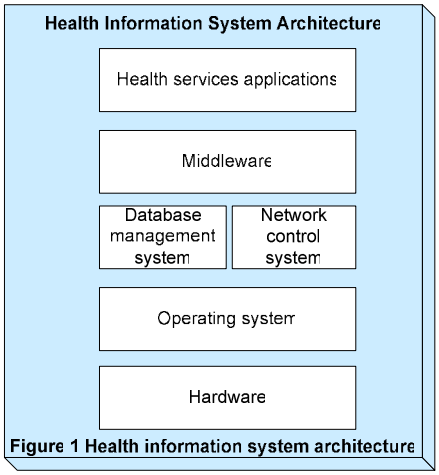

Figure 1 Health information system architecture

Security may be implemented at the level of the health services applications system. However, even if security is established within that health service system, the overall system can be no more secure than the operating system upon which the applications depend. The operating system itself can be no more secure than the hardware facilities of the computer on which the operating system performs. Likewise, any other software component set, such as “middleware”, database management system (DBMS), network interface structure or “stack”, etc. is constructed above the operating system and so totally depend upon security functions provided by the operating system as well as the robustness of that OS against attack.

Necessary healthcare security services such as authentication, authorisation, data privacy and data integrity can only be confidently assured when the operating system is trusted. Thus “trusted operating systems” provide the foundation for any security and privacy schemes required. Such strong security platforms may be considered as necessary to ensure the protection of electronic health information from both internal and external threats as well as providing conformance of health information systems to regulatory and legal requirements.

Loscocco et al [27] have stated that the underlying operating system should be responsible for protecting the “application-space” against tampering, bypassing and spoofing attacks. They address the significance of secure operating systems as follows:

> *“The threats posed by the modern computing environment cannot be addressed without support from secure operating systems and any security effort which ignores this fact can only result in a “fortress built upon sand.”*

It is an inherently insecure exercise to attempt to build an application requiring high levels of trust in the maintenance of security and privacy when the underlying structure within a computer system is a non-trusted operating system. Simply put, the trusted application relies totally upon the non-trusted operating system to access low level services.

This analysis indicates that not only is a new level of security required in healthcare related information systems, based around MAC/LSPP structures but also that appropriate “chief information officers (CIOs)” and systems designers are educated, trained and experienced

Proceedings of the National e-Health Privacy and Security Symposium 2006 (ehPASS'06) - ISBN: 1741071380 © 2006 QUT.

in such systems. This would appear to present the major challenge to privacy and security in e-health information systems for at least the next 5 years.

References

[1] NHS, The Use Of Computers In Health Care Can Reduce Errors, Improve Patient Safety, And Enhance The Quality Of Service - There Is Evidence http://www.connectingforhealth.nhs.uk/worldview/protti2/, accessed 17/08/2006

[2] Goldschmidt, P.G., *HIT and MIS: Implications of Health Information Technology and Medical Information Systems.* Communications of the ACM, 2005. **48**(10): p. 69-74.

[3] Carter, M., Integrated Electronic Health Records and Patient Privacy: Possible Benefits but Real Dangers http://www.mja.com.au/public/issues/172_01_030100/carter/carter.html#subr0, accessed 17/07/2005

[4] HHS, HIPAA Administrative Simplification Regulation Text 45 CFR Parts 160, 162, and (Unofficial Version, as amended through February 16, 2006) http://www.hhs.gov/ocr/AdminSimpRegText.pdf, accessed 10/06/2006

[5] HHS, Information Security Program Health Insurance Portability and Accountability Act (HIPAA) Compliance Guide [September 14, 2005] http://csrc.nist.gov/fasp/FASPDocs/program-mgmt/HHS_HIPAA_Compliance_Guide_09142005.pdf, accessed 15/06/2006

[6] HHS, HIPAA Administrative Simplification Compliance Deadlines http://www.cms.hhs.gov/HIPAAGenInfo/Downloads/HIPAAComplianceDeadlines.pdf, accessed 12/06/2006

[7] Beaver, K. and R. Herold, *The Practical Guide to HIPAA Privacy and Security Compliance*. 2004: Auerbach Publications.

[8] HHS, 45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards: Final Rule (Federal Register / Vol. 68 No. 34 / Thursday, February 20, 2003 / Rules and Regulations) http://aspe.hhs.gov/admnismp/FINAL/Fr03-8334.pdf, accessed 10/06/2006

[9] *Privacy Act 1988*. 1988.

[10] OFPC, Federal Privacy Law http://www.privacy.gov.au/act/index.html, accessed 26/07/2006

[11] OFPC, Guidelines to the National Privacy Principles http://www.privacy.gov.au/publications/nppgl_01.html, accessed 27/07/2006

[12] NHMRC, Guidelines Under Section 95 of the Privacy Act 1988 http://www.privacy.gov.au/publications/e26.pdf, accessed 30/07/2006

[13] NHMRC, Guidelines approved under Section 95A of the Privacy Act 1988 http://www.nhmrc.gov.au/publications/_files/e43.pdf, accessed 30/07/2006

[14] Fernando, J., *Factors that have Contributed to a Lack of Integration in Health Information System Security.* The Journal on Information Technology in Healthcare, 2004. **2**(5): p. 313-328.

[15] DoHA, The Proposed National Health Privacy Code http://www7.health.gov.au/pubs/nhpcode.htm, accessed 11/07/2005

[16] DoD, *Trusted Computer System Evaluation Criteria (TCSEC), DoD 5200.28-STD*. 1985, Department of Defense.

[17] ITSEC, *Information Technology Security Evaluation Criteria, Version 1.2*. 1991, Office for Official Publications of the European Communities.

[18] CC, *Common Criteria for Information Technology Security Evaluation Draft Version 3.0*. 2005.

[19] Merkow, M.S. and J. Breithaupt, *Computer Security Assurance Using The Common Criteria*. 2005: Thomson Delmar Learning.

[20] Shapiro, J.S., *Understanding the Widnows EAL4 Evaluation.* IEEE Computer Society Press, 2003. **36**(2): p. 103-105.

Proceedings of the National e-Health Privacy and Security Symposium 2006 (ehPASS'06) - ISBN: 1741071380 © 2006 QUT.

[21] NSA, Controlled Access Protection Profile Version 1.d http://niap.nist.gov/cc-scheme/pp/PP_CAPP_V1.d.pdf, accessed 18/10/2005
[22] NSA, Lablled Security Protestion Profile Version 1b http://niap.nist.gov/cc-scheme/pp/PP_LSPP_V1.b.pdf, accessed 18/10/2005
[23] Reynolds, J. and R. Chandramouli, Role-Based Access Control Protection Profile Version 1.0 http://www.cesg.gov.uk/site/iacs/itsec/media/protection-profiles/RBAC_987.pdf, accessed 18/10/2005
[24] BSI, Common Criteria Protection Profile electronic Health Card (eHC) – elektronische Gesundheitskarte (eGK) http://www.bsi.de/zertifiz/zert/reporte/PP0020b.pdf, accessed 08/08/2006
[25] BSI, Common Criteria Protection Profile Health Professional Card (HPC) Heilberufsausweis (HPA) http://www.bsi.de/zertifiz/zert/reporte/PP0018b.pdf, accessed 08/08/2006
[26] TNOITSEF, Developers | list of evaluated products http://www.commoncriteriaportal.org/public/developer/index.php, accessed 08/08/2006
[27] Loscocco, P., et al. *The Inevitability of Failure: The Flawed Assumption of Security in Modern Computing Environments*. in *Proceedings of the 21st National Information Systems Security Conference*. 1998.

Acknowledgements

The authors would like to thank Professor Peter Croll for his continuous and welcome advice and recommendation in regard to this paper.