AN ARCHITECTURE FOR ENHANCED ASSURANCE IN E-HEALTH SYSTEMS

Yin-Miao Vicky Liu
Bachelor of Business Computing, QUT 1993
Master of Information Technology (Research), QUT 2005

Information Security Institute
Faculty of Science and Technology
Queensland University of Technology

A thesis submitted to the Queensland University of Technology
in accordance with the regulations for
Degree of Doctor of Philosophy

May 2011

Declaration

The work contained in this thesis has not been submitted for a degree or diploma at any other higher education institution. To the best of my knowledge and belief, this thesis contains no material previously published or written by another person except where due reference is made.

Signature :

Date:

Abstract

Notwithstanding the obvious potential advantages of information and communications technology (ICT) in the enhanced provision of healthcare services, there are some concerns associated with integration of and access to electronic health records. A security violation in health records, such as an unauthorised disclosure or unauthorised alteration of an individual's health information, can significantly undermine both healthcare providers' and consumers' confidence and trust in e-health systems. A crisis in confidence in any national level e-health system could seriously degrade the realisation of the system's potential benefits.

In response to the privacy and security requirements for the protection of health information, this research project investigated national and international e-health development activities to identify the necessary requirements for the creation of a trusted health information system architecture consistent with legislative and regulatory requirements and relevant health informatics standards. The research examined the appropriateness and sustainability of the current approaches for the protection of health information. It then proposed an architecture to facilitate the viable and sustainable enforcement of privacy and security in health information systems under the project title "Open and Trusted Health Information Systems (OTHIS)". OTHIS addresses necessary security controls to protect sensitive health information when such data is at rest, during processing and in transit with three separate and achievable security function-based concepts and modules: a) Health Informatics Application Security (HIAS); b) Health Informatics Access Control (HIAC); and c) Health Informatics Network Security (HINS).

The outcome of this research is a roadmap for a viable and sustainable architecture for providing robust protection and security of health information including elucidations of three achievable security control subsystem requirements within the proposed architecture. The successful completion of two proof-of-concept prototypes demonstrated the comprehensibility, feasibility and practicality of the HIAC and HIAS models for the development

and assessment of trusted health systems. Meanwhile, the OTHIS architecture has provided guidance for technical and security design appropriate to the development and implementation of trusted health information systems whilst simultaneously offering guidance for ongoing research projects. The socio-economic implications of this research can be summarised in the fact that this research embraces the need for low cost security strategies against economic realities by using open-source technologies for overall test implementation. This allows the proposed architecture to be publicly accessible, providing a platform for interoperability to meet real-world application security demands. On the whole, the OTHIS architecture sets a high level of security standard for the establishment and maintenance of both current and future health information systems. This thereby increases healthcare providers' and consumers' trust in the adoption of electronic health records to realise the associated benefits.

Keyword:

security architecture of health information systems, security for health systems, security in health informatics

Acknowledgements

This study would not have been possible without those who assisted and guided me in various ways through the course of this research project. I would like to express my deepest and most sincere appreciation to them.

I would like to thank my Principal Supervisor, Professor Emeritus William (Bill) Caelli, AO, for his wealth of knowledge and experience in information security, marvellous guidance, and tremendous support. Indeed, it has been a privilege and a pleasure to undertake my masters by research and PhD studies under his guidance and supervision. Professor Caelli plays such an active role in the national and international information security community, in particular, his passions in research to educate people and to share his incredible wealth of wisdom. I would like thank my former Associate Supervisor Dr. Lauren May for providing invaluable advice, guidance and constant encouragement throughout this research. I also thank my Associate Supervisor, Adjunct Associate Professor Jason Smith for his guidance to this study. My gratitude goes to my former Associate Supervisor Professor Peter Croll for his insightful advice particularly during the early stages of the development of the architectural concept and the creation and demonstration of the SELinux-based system. I would like to express my appreciation to Ms. Rachel Cobcroft for her meticulous and professional editing work on this thesis.

I am most grateful for the wonderful support and understanding from my mother, sister, and dear friends. I would like to give special thanks to Sr. Uriela Emm for her continuous encouragement and friendship that has been such a vital strength throughout this study. My gratitude goes to Dr. Taizan Chan for his kind wishes and encouragement at all times. Last but not least, my heartfelt thanksgiving goes to my God for the provision, strength, wisdom, and understanding needed for this journey.

Table of Contents

List of Figures

List of Tables

Chapter 1 Research Overview

1.1 Description of the research problem investigated

In the 21st century, Information and Communications Technology (ICT) and its artefacts provide the critical infrastructure needed to support most essential services, including the information services of the healthcare sector. The use of computer-based information systems and associated telecommunications and data network infrastructure to process, transmit, and store health information plays an increasingly significant role in the improvement of quality and productivity in healthcare.

Despite e-health's potential to improve the processing of health data, electronic health records may inadvertently pose new threats to the protection of sensitive health data, if not designed and managed effectively. Moreover, e-health's basic confidentiality, integrity, and availability parameters must be considered from its earliest research and development stages. Malevolent motivations in both internal system users and external attackers of the system could result in disclosure of confidential personal health information on a widespread scale, and at a higher speed than possible with traditional paper-based medical records. Unlike other industries and enterprises, such as the banking and finance sectors, loss of privacy through disclosure of health record data is normally not recoverable. Namely, unlike the banking sector, a new account cannot be created along with all other necessary identification and authentication data and processes. Health data is usually "locked" to an individual. Security violations in health information systems, such as an unauthorised disclosure or unauthorised alteration of individual health information, therefore have the potential for disaster among healthcare providers and consumers.

There are some major concerns associated with the integration of, and access to, electronic health records. Information stored within electronic health systems is highly sensitive by its very nature. The management of

health records, therefore, carries clear requirements for the protection of health record confidentiality and the maintenance of integrity.

This research addresses the shortcomings surrounding privacy and security of contemporary ICT systems for the protection of sensitive health information. The key research question investigated and reported upon in this thesis is summarised as follows:

> Are current approaches to the protection of the security of health information systems appropriate and sustainable? If not, is it possible to create a suitable trusted system architecture for security and control, with associated management functions at each level in a health information system, while maintaining a holistic approach to the problem?

This research proposes a secure system architecture for a health information system that consists of a set of achievable security control modules. This study was performed and results obtained as to whether this proposed architecture is a viable, sustainable, and holistic approach to provide adequate levels of security protection for health information systems.

1.2 The overall objectives of the study

In response to the health sector's privacy and security requirements for contemporary health information systems, the overall goal of this research is to propose a feasible and sustainable solution to meeting security demands using open architecture, available technologies, and open standards. A trusted and open system architecture is therefore needed to address the privacy protection and security for health systems in a holistic and end-to-end manner, and not one that involves just the data communications level using securing messaging technology alone.

1.3 The specific aims of the study

To address privacy and security requirements at each level within a modern health information system, this research has aimed:

1. To investigate electronic health management applications and deployment activities, nationally and internationally;
2. To identify the necessary requirements and constraints for the creation of any possible trusted information system architecture consistent with health regulatory requirements and standards;
3. To examine the appropriateness and sustainability of the current approaches for the protection of sensitive electronic patient data;
4. To propose a viable, open, and trusted architecture for health information systems comprised of a set of separate but achievable security control modules building on top of a trusted platform;
5. To develop a viable and sustainable approach to the provision of appropriate levels of secure access control management for the protection of sensitive health data;
6. To provide advice on the necessary security controls for the Network and Application Levels to protect sensitive health information in transit and under processing; and
7. To present the practicality, feasibility, clarity, and comprehensibility of the proposed network security architecture for enabling the ready development of systems based on the overall architecture through the demonstration and analysis of a small experimental system.

The relevance of each specific aim above is validated through the six published papers included in this thesis, as follows:

- Chapter 3 substantiates the relevance of Aims 1 and 2;
- Chapter 4 confirms the relevance of Aim 3;
- Chapter 5 supports the relevance of Aim 4;
- Chapter 6 authenticates the relevance of Aim 5;
- Chapter 7 strongly supports the relevance of Aim 6; and
- Chapter 8 verifies the relevance of Aim 7.

1.4 An account of research progress linking the research papers

In order to address the security requirements for a trustworthy e-health system in a holistic manner, the thesis proposes the Open and Trusted Health Information Systems (OTHIS). OTHIS is an open architecture espousing open standards and open-source technologies rather than utilising proprietary technologies. As illustrated in Figure 1, OTHIS architecture aims at building firmware and hardware bases on top of trusted operating systems, to provide a solid security foundation for any secure and trusted health information system. Without a trusted computing base, any system is subject to compromise. Necessary healthcare security services such as authentication, authorisation, data privacy, and data integrity can only be confidently assured when the system foundation is trusted. Such strong security platforms are considered 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.

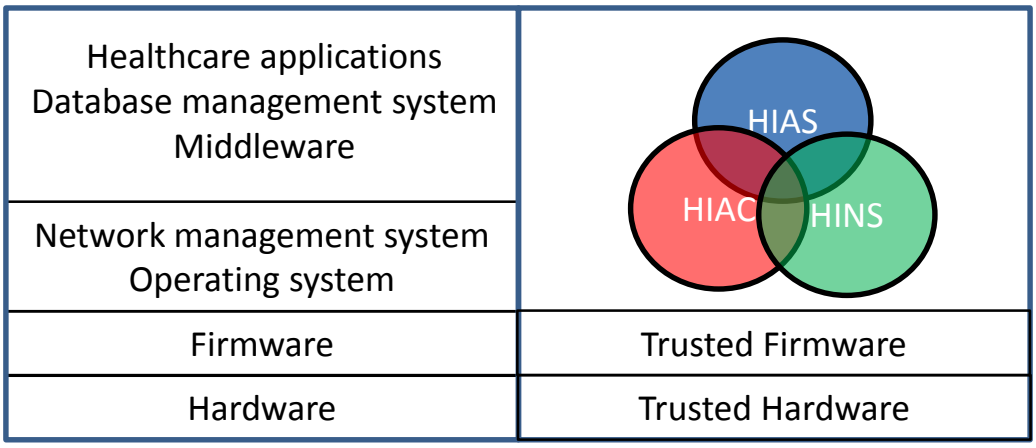


Figure 1 Open Trusted Health Information Systems (OTHIS)

OTHIS is a modularised architecture for health information systems, consisting of three separate and achievable function-based modules:

- Health Informatics Access Control (HIAC): HIAC aims at addressing a far finer level of granularity needed for verifiable security and control management requirements in a health information system,

from the network, operating system, and database management system (data accessibility at table/view, row/column, and cell levels in databases) up to the Application Layer.

- Health Informatics Application Security (HIAS): HIAS aims at addressing data protection requirements which are reflected in law and associated regulatory instruments. This is achieved through practical security services provided by healthcare applications at the data element level through to security provisions at any service level. Thus, HIAS could cater for situations where Web Services-based applications and Health Level 7 (HL7) messaging and data transfer structures are being used as the major health information transport methodology. It aims at achieving this in a trusted, secure, and efficient manner.
- Health Informatics Network Security (HINS): HINS consists of the appropriate Network Level security structure within a distributed health system. HINS is aimed at the provision of services and mechanisms to authenticate claims of identity, to provide appropriate authorisations following authentication, to prevent unauthorised access to shared health data, to protect the network from attacks, and to provide secure communications services for health data transmission over open data networks.

Figure 2 illustrates the relevance of the papers forming the basis of this thesis. These consist of five conference papers, and one journal publication.

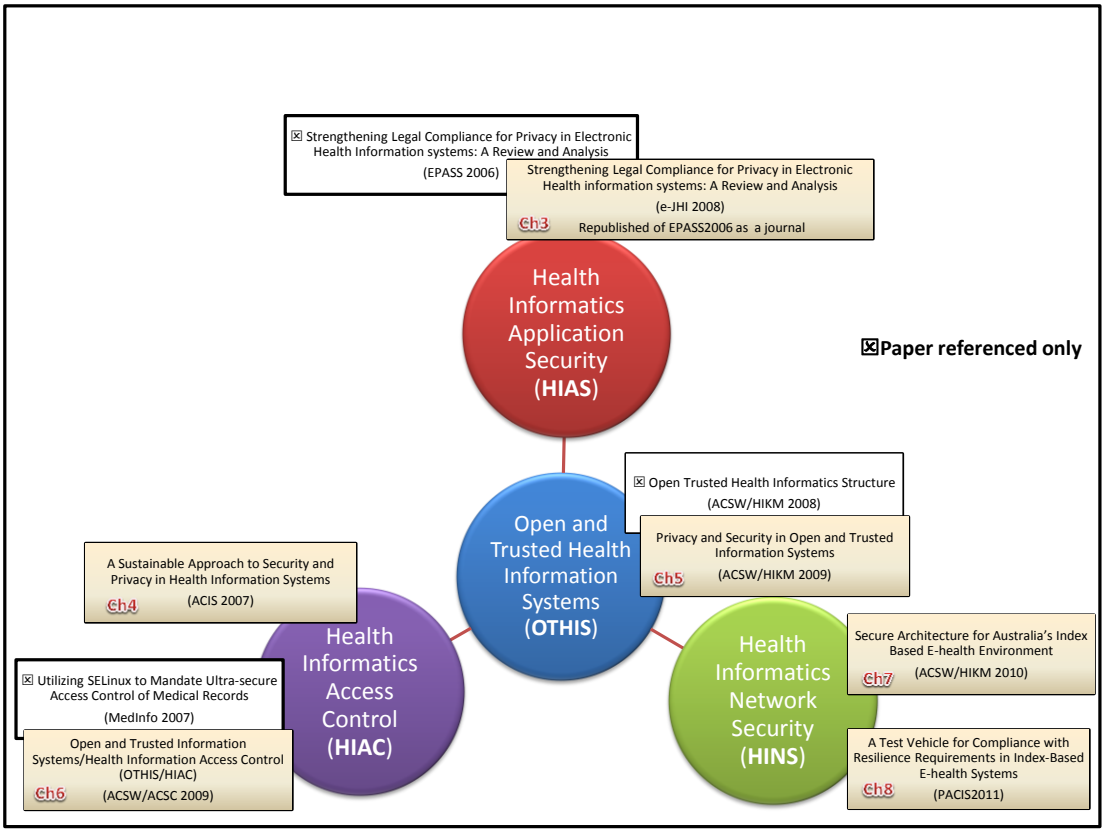


Figure 2: Publications linked to the research theme

1.4.1 Chapter 3: Strengthening Legal Compliance for Privacy in Electronic Health Information Systems: A Review and Analysis

This research activity has provided the relevant information for determining the requirements for, and constraints on, the creation of any trusted information system architecture for an electronic health system. Chapter 3 investigates electronic health management applications and deployment activities at both national and international levels. It also analyses the required access management in health informatics in the United States of America and Australia.

In developing a new approach to the electronic health management application, it is necessary to be aware of issues identified with current and previous attempts to implement e-health activities at both national and international levels. There are lessons to be drawn from international experience in e-health development and implementation. This analysis also gives a perspective on "real-world" and current issues which need to be

addressed. Regardless of the location of the actual health system application, be it in the UK, USA, or Australia, common inherent requirements in any health information system are the ability to provide security and privacy features as and where required.

It has been essential to review the USA's laws with regard to the protection of health information, as well as to explore Australian Federal, State, and Territory legislation, policies, and standards. The USA's *Health Insurance Portability and Accountability Act (HIPAA) 1996* provisions may have widespread influence on the entire healthcare industry worldwide. This is in addition to having an immediate impact on every information system that uses or processes health information in the USA. This chapter also investigates the Australian *Federal Privacy Act 1988*, and jurisdictional State and Territory privacy and health record laws.

1.4.2 Chapter 4: A Sustainable Approach to Security and Privacy in Health Information Systems

In examining the appropriateness and sustainability of the current approaches for the protection of sensitive patient data, Chapter 4 identifies and discusses recent information security violations or weaknesses found in national infrastructure in Australia, the UK, and the USA; two of which involve departments of health and social services. These three illustrated cases all have a common security weakness which directly relates to access control management. Appropriate computer-based access control schemes can be deployed to address these information security issues.

Again, from an information security perspective, this chapter also investigates major access control models. It argues that a radical re-think is absolutely crucial to the understanding of access control technologies and implementations in light of modern information system structures, legislative and regulatory requirements, and overall security demands on operational health information systems. This chapter proposes a viable and sustainable approach to the provision of appropriate levels of secure access control management under an overall trusted health informatics scheme, with a focus on trustworthy access control mechanisms. This research therefore

proposes the “Health Informatics Access Control (HIAC)” model within the overall “Open and Trusted Health Information System (OTHIS)” concept. The aim is to overcome privacy and security issues which have plagued previous attempts to advance security structures in electronic health management systems. To determine the practical viability of a HIAC model for health systems, this chapter reports on a HIAC proof-of-concept prototype which was built to exploit the enhanced security features of a current trusted operating system which, in some implementations, has been evaluated under the “Common Criteria” (international standard IS15408) paradigm. Namely, it was built on the Security Enhanced Linux (SELinux) structures in the Red Hat Enterprise Linux (RHEL) Version 4 operating system.

1.4.3 Chapter 5: Privacy and Security in Open and Trusted Health Information Systems

The initial OTHIS scheme is introduced broadly in Chapter 4 in response to the health sector’s privacy and security requirements for a contemporary health information system. Chapter 5 addresses the OTHIS philosophy and architecture components.

The OTHIS philosophy aims to achieve a high level of information assurance in health information systems. As such, the OTHIS scheme is proposed as a holistic approach to address privacy and security requirements at each level of a modern health information system. The aim is to ensure the protection of data from both internal and external threats. OTHIS, it is believed, has the capacity to ensure the legal compliance of any health information system to appropriate legislative and regulatory requirements. In line with contemporary concepts of open-source information technologies, OTHIS incorporates the term “open” to embrace relevant open architectures and allied technical standards. Therefore, open-source technologies and software products are used rather than proprietary technologies. OTHIS also incorporates the term “trusted system.” Without a relevant trusted computing base (TCB), any system is subject to compromise. In particular, data security at the Application Level can be assured only when the healthcare application is operating on top of a TCB-oriented platform. This applies to all healthcare

applications and related databases to achieve adequate information assurance. For this reason, OTHIS aims at overall application systems running on top of trusted systems software, middleware, firmware, and hardware bases.

OTHIS is a modularised architecture for health information systems. Each module has a specific focus area. There is inevitably some overlap across those modules, however. As stated previously, OTHIS consists of three separate and achievable function-based modules:

- HIAC;
- HIAS; and
- HINS.

1.4.4 Chapter 6: Open and Trusted Health Information Systems/Health Informatics Access Control (OTHIS/HIAC)

Chapter 6 reviews the HIAC proof-of-concept prototype developed under the overall OTHIS architecture (in Chapter 5) to exemplify improved flexibility via SELinux policy configurations. This chapter illustrates the key SELinux concepts and procedures for developing a security policy using SELinux security mechanisms to protect sensitive health data stored and processed in health information systems. This is coupled with an example coding of the SELinux policy configurations.

In Chapter 4, the HIAC proof-of-concept prototype was developed at the early stages of the overall SELinux operating system project development. It was argued that previous SELinux mandatory access policy development and management facilities were too inflexible to handle a large-scale health system efficiently, which may involve dynamic and frequent changes to security policies, such as adding/deleting users and applications. With the earlier SELinux distribution, any changes and extensions made to an SELinux system access policy would have required the source policy coding to be recompiled and the system to be restarted. As SELinux has continued to advance and evolve, any changes to those security policies can be recompiled with available tools and techniques. Updated security polices can

then be reloaded into the system kernel without the need to restart the system. To date, the HIAC proof-of-concept prototype has been updated to the Fedora Core 9 operating system distribution. This has been used to confirm the flexibility of SELinux in providing the levels of assurance required.

Increasingly, health information systems are being developed and deployed based upon commercial, commodity-level ICT productions and systems, commonly referred to as “Commercial Off-the-Shelf (COTS) Systems.” Such general-purpose systems have been created over the last 25 years with often only minimal security functionality and verification. In particular, access control at the operating system level performs a vital security function in protecting sensitive application packages. Contemporary access control builds on the earlier method known as “Discretionary Access Control (DAC)”.

The DAC structure is widely implemented to manage overall system access control in current commodity software such as Microsoft Corporation’s Windows systems, open-source systems such as Linux, and the original Unix system. Applications that rely on DAC mechanisms are vulnerable to tampering and bypassing and normally do not allow for mandatory labelling of all system “objects”. Malicious or flawed applications can easily cause security violations in the DAC environment. This environment alone is no longer valid for modern health information systems and, when used, is normally supplemented by Application and Network Layer security services and mechanisms. HIAC provides a flexible form of a Mandatory Access Control (Flexible MAC) model, accompanied, as is the norm, by Role-Based Access Control (RBAC) properties to simplify authorisation management. This degree of simultaneous control, flexibility, and a refined level of granularity is not achievable with DAC, RBAC, or even MAC individually.

This chapter argues that adoption of appropriate security technologies, in particular Flexible MAC-oriented operating system bases, can satisfy the requirements for the protection of sensitive health data, as the HIAC model has demonstrated.

1.4.5 Chapter 7: A Secure Architecture for Australia's Index-Based E-health Environment

Generally, health information is stored over a number of different computer systems under diverse management regimes working at different levels, such as geographic, enterprise, and so forth. For the provision of national level healthcare information services at both patient and healthcare provider levels, a national index system must be available for the provision of directory services to determine the distributed locations of the source systems holding the related health records. Chapter 7 addresses this need by proposing a connectivity architecture with the required structures to support secure communications between healthcare providers and the Index System in the national e-health environment, including:

- The Index System itself; and
- The proposed Healthcare Interface Processor (HIP) module.

The Index System, a centralised facility run at a national level, should be built on a high-trust computer platform to perform authentication and indexing services. This proposal draws on important lessons from the Internet's Domain Name System (DNS) for the development and deployment of the national healthcare Index System. Particularly, the chapter argues that a fundamental security issue, that of name resolution, must be addressed prior to the initiation of interactions between the healthcare providers and national Index System. This chapter, therefore, proposes a trusted architecture not only providing the indexing service but also incorporating a trusted name resolution scheme for the enforcement of communicating to the authorised Index System.

This thesis' design philosophy of HIP draws on principles used in the original "Interface Message Processor (IMP)" system of the Advanced Research Projects Agency Network (ARPANET), to isolate the disparate "downstream" systems and associated networks of users connected to the ARPANET network. The design rationale underlying HIP, a resilient and qualified facility built on top of a trusted base-embedded hardware and software platform, is

to act as a proxy server to establish a secured communication channel connecting to the Index System and for health information exchange between healthcare providers. This design could isolate a potentially hostile or compromising system connected to the national e-health network. Wherever a connection to the national indexing system is required, a HIP facility has to exist in some form. HIP carries out its work from Layers 1 to 7 of the ISO OSI model to achieve security provisions based upon the original and seminal ISO 7498-2 interconnection security model. Its aims are:

- To establish a trusted path to connect to the authorised Index System;
- To provide peer-entity authentication between healthcare providers and national Index System;
- To facilitate secure healthcare information exchange in transit;
- To provide data protection with appropriate access control mechanisms;
- To provide messaging interoperability to enable healthcare information exchange between disparate health systems with incorporation of an HL7 Interface Engine and Message Mapping Sets; and
- To provide operation flexibility with “emergency override” and capacity flexibility for various scales of healthcare organisations.

The HIP may therefore be seen as being responsible for providing all necessary protocol conversion, network management, and security functions. The security service provisions listed above, and incorporated into the HIP, have the potential to achieve the stated goals of HINS, HIAS, and HIAC within the proposed OTHIS scheme.

This proposed architecture is based on the broad architecture of the Australian Government’s National E-Health Strategy and Connectivity Architecture, outlined by the National E-Health Transition Authority (NEHTA). Although this proposal focuses on the Australian national e-health environment, this design could be equally applied to any distributed, index-

based healthcare information system involving cross-referencing of disparate health data collections or repositories.

1.4.6 Chapter 8: A Test Vehicle for Compliance with Resilience Requirements in Index-based E-health Systems

To demonstrate the practicality, feasibility, clarity, and comprehensibility of the proposed security architecture, this chapter presents evidence for these ICT system development requirements through the creation of an experimental demonstration system applied to index-based e-health environments. This experiment was performed against the definition of a minimalistic e-health systems environment, consisting of a national Index System and three participating healthcare entities. This prototype development was implemented as a university postgraduate student project with approximately 288 hours of development effort involved. This included the time required to obtain an understanding of the architecture and system specifications, exploring and selecting development tool sets, coding, testing, debugging, and system documentation.

The successful completion of this prototype demonstrated the comprehensibility of the proposed architecture, as well as the clarity and feasibility of system specifications. These factors enabled ready development of a small test system. As demonstrated, the creation of such a system does not require high levels of specialised system development knowledge and expertise. The outcome of this test vehicle is beneficial in providing a logic process model of, and functional specifications for, the proposed security architecture for index-based e-health systems. It provides a practical aid in the development of guidelines and the assessment of functional conformance of implementations.

This test vehicle has indicated a number of parameters that need to be considered in any national index-based e-health system design with reasonable levels of system security. This chapter identifies the need for evaluation of the areas and the levels of education, training, and expertise needed by ICT professionals to create such a system. Essentially, this

chapter verifies the feasibility of the OTHIS scheme proposed and the relevance of this thesis research.

1.5 Research Scope

In health informatics, research themes may cover a broad spectrum of concepts and technologies. These include clinical terminologies, various structure and content standards in electronic health records, and messaging standards for health information exchange. They also embrace clinical knowledge management systems and telemedicine healthcare and health system architectures. This research theme is related to health system architecture from a security perspective, with a focus on health data under processing, in transit, and at rest.

The research processes used have been naturally constrained by available academic resources within the research facilities at the Faculty of Science and Technology (FaST) of the Queensland University of Technology (QUT). The methodology used, therefore, consists of the proposal, definition, analysis, and preliminary testing of a very small prototype of an overall secure information system structure for an e-health record indexing system.

1.6 Research contributions and outcomes

The overall work reported in this thesis, with its associated set of papers, demonstrates the contribution made to the Information Systems (IS) discipline and, in particular, to the area of secure information systems and services in the e-health arena. It achieves this through a clear articulation of a broad architecture for such systems, coupled with detailed explanations of each of the components.

Some socio-economic implications gleaned from this research and of interest to the healthcare sector are:

- The research successfully embraced low-cost security strategies;
- Recognition of economic realities that are vital to success.

These parameters were explored through the use of open-source technologies and products for implementation of test systems, rather than high-cost proprietary products and systems. This also allows the architecture to be publicly accessible, providing a platform for interoperability to meet real-world application security demands. This proposed architecture also sets a high level for security standards in the establishment and maintenance of both current and future large-scale health information systems. It thereby increases healthcare providers' and consumers' trust in the adoption of electronic health records to realise any associated benefits.

The outcome of this research is a roadmap of a viable and sustainable architecture for providing robust protection and security of health information. It includes explanations of three achievable security control subsystem requirements within the proposed architecture. The successful completion of two proof-of-concept prototypes demonstrates the comprehensibility, feasibility, and practicality of the HIAC and HINS models for the development and assessment of trusted health systems.

Meanwhile, the OTHIS Research Group has been formed to promote the OTHIS architecture that provides guidance for technical and security design appropriate to the development and implementation of trusted health information systems. This research group and its associated program of work intends to provide a sufficiently rich set of security controls that satisfies the breadth and depth of security requirements for health information systems, whilst simultaneously offering guidance to ongoing research projects.

1.7 Thesis Format

For uniformity of presentation, the published papers forming the basis of this thesis are presented in their original word-processing form as submitted to the associated conferences and journals.

1.8 Thesis Structure

This thesis comprises the following chapters:

- Chapter 1: Research Overview
- Chapter 2: Literature Review
- Chapter 3: Strengthening Legal Compliance for Privacy in Electronic Health Information Systems: A Review and Analysis
- Chapter 4: A Sustainable Approach to Security and Privacy in Health Information Systems
- Chapter 5: Privacy and Security in Open and Trusted Health Information Systems
- Chapter 6: Open and Trusted Health Information Systems/Health Informatics Access Control (OTHIS/HIAC)
- Chapter 7: A Secure Architecture for Australia's Index-Based E-health Environment
- Chapter 8: A Test Vehicle for Compliance with Resilience Requirements in Index-Based E-health Systems
- Chapter 9: General Discussion

1.9 List of Publications

The following publications and manuscripts are included in, and incorporated into, this thesis:

Chapter 3:
V. Liu, W. Caelli, L. May, P. Croll, Strengthening Legal Compliance for Privacy in Electronic Health Information Systems: A Review and Analysis. The Electronic Journal of Health Informatics (eJHI), 2008. Vol 3 (1: e3)

Chapter 4:
V. Liu, W. Caelli, L. May, P. Croll, A Sustainable Approach to Security and Privacy in Health Information Systems, appeared in: 18th Australasian Conference on Information Systems (ACIS) Toowoomba, Australia, (2007)

Chapter 5:
V. Liu, W. Caelli, L. May, T. Sahama, Privacy and Security in Open and Trusted Health Information Systems, appeared in: Third Australasian

Workshop on Health Informatics and Knowledge Management (HIKM 2009). Wellington, New Zealand, (2009) Vol. 97

Chapter 6:
V. Liu, L. Franco, W. Caelli, L. May, T. Sahama, Open and Trusted Information Systems/Health Informatics Access Control (OTHIS/HIAC), appeared in: the 32nd Australasian Computer Science Conference (ACSC 2009). Wellington, New Zealand, (2009), Conferences in Research and Practice in Information Technology (CRPIT), Vol. 98.

Chapter 7:
V. Liu, W. Caelli, J. Smith, L. May, M. Lee, Z. Ng, J. Foo, W. Li, Secure Architecture for Australia's Index Based E-health Environment appeared in: The Australasian Workshop on Health Informatics and Knowledge Management in conjunction with the 33rd Australasian Computer Science Conference Brisbane, Australia, (2010) Vol. 108

Chapter 8:
V. Liu, W. Caelli, Y. Yang L. May, A Test Vehicle for Compliance with Resilience Requirements in Index-based E-health Systems is to appear at the 15th Pacific Asia Conference on Information systems (PACIS) in 7-11 July 2011 Brisbane, Australia.

Other publications by the candidate are as follows:

V. Liu, W. Caelli, L. May, Strengthening Legal Compliance for Privacy in Electronic Health Information Systems: A Review and Analysis, in: National e-Health Privacy and Security Symposium, ehPASS'06. Queensland University of Technology, Brisbane, Australia (2006).

P. Croll, M. Henricksen, W. Caelli, V. Liu, Utilizing SELinux to Mandate Ultra-secure Access Control of Medical Records, appeared in: 12th World Congress on Health (Medical) Informatics, Medinfo2007. Brisbane Australia, (2007).

V. Liu, W. Caelli, L. May, P. Croll, Open Trusted Health Informatics Structure, appeared in: Australasian Workshop on Health Data and Knowledge

Management, the Australian Computer Science Week Wollongong Australia: ACM (2008).

1.10 Individual Contribution

The candidate was the principal investigator throughout the period of research covered in this thesis. This activity involved:

- Development and definition of the overall security concept and architecture;
- Identification of all necessary subsystems and components; and
- Definition and development of proof-of-concept activities in both an application development environment (Chapter 8) and in the structural definition and management assessment of the security architecture in a specialised (SELinux) environment (Chapter 6).

In particular, the candidate is the principal author of the six publications submitted as the components of this thesis as well as the other related chapters therein. All acquisition, analysis, and interpretation of data obtained have also been undertaken by the candidate.

Chapter 2 Literature Review

The purpose of this chapter is to provide a critical review of relevant literature, to identify knowledge gaps, and to identify the relationship of the literature to this research. This chapter begins with an emphasis on the significance of security and privacy protection for health information systems, since these elements play a significant role in the successful implementation of a national electronic health system. The Open and Trusted Health Information Systems (OTHIS) architecture proposed in this thesis is aimed at fulfilling the security requirements for health information systems. This chapter explores and analyses a number of national e-health initiatives, including those in Australia, Canada, England, Germany, the Netherlands and the USA.

The security services and requirements for health information systems can be categorised into access control management, application security, and communication security. This chapter discusses these three types of security measures. In developing a trusted and interoperable health information system architecture, it is essential to study the national and international standards and specifications related to security architectures for electronic health record systems. This chapter also includes exemplary instruments used in health information systems. Finally, the chapter concludes with the limitations of existing approaches. It should be noted that this literature review has been conducted up to 30 June 2010.

2.1 The significance of the security protection for health information systems

Undoubtedly, the adoption of e-health has much potential to improve healthcare delivery and performance. Anticipated improvements relate to better management and coordination of healthcare information and increased quality and safety of healthcare delivery. A security violation in health records, such as an unauthorised disclosure or unauthorised alteration of an individual's health information, can significantly undermine both healthcare providers' and consumers' confidence and trust in e-health

systems. A crisis in confidence in national e-health systems would seriously degrade the realisation of the system's potential benefits.

A number of papers [1-13] have been written espousing the importance of the security and privacy provisions of health information systems. For example, Blobel et al. [9] emphasise that security and privacy services must be the integral part of a trustworthy health information system. Tsiknakis et al. [12] state that the trust and security infrastructure of a health information network is an important factor influencing user adoption. Goldschmidt [5] points out that malevolent parties could feasibly disclose confidential electronic health records on a more widespread scale. Of particular note is survey evidence from the Australia's National E-health Transition Authority (NEHTA) in the *Privacy Blueprint for the Individual Electronic Health Record Report on Feedback* [2]. This report was released for public comment in 2008, with 37 submissions received in total. The findings of this report indicate that numerous healthcare consumers and providers welcome the adoption of national individual electronic health records because of the potential benefits. There are also a number of consumers, however, who are reluctant to embrace e-health owing to privacy concerns. Clearly, the protection of information security and privacy is critical to the successful implementation of any e-health initiative. NEHTA therefore places security and privacy protection at the centre of its e-health approach.

In the case of the United Kingdom, its National Health Service (NHS) [14] requires that all reasonable safeguards be implemented to prevent inappropriate access, unauthorised modification, or manipulation of sensitive patient records.

The United States' *Health Insurance Portability and Accountability Act (HIPAA) 1966* [15-20] was enacted by the United States Congress to address numerous healthcare-related topics. The purpose of HIPAA provisions is to encourage electronic health transactions while requiring safeguards to protect the security and privacy of health information. The Act includes the Security Rule and the Privacy Rule, which stipulate security requirements relevant to the implementation of security controls in any health

information system. The USA's HIPAA provisions have widespread implications for the global healthcare industry, in addition to having an immediate effect on every information system that uses or processes health information in the USA.

2.2 Overall national e-health architectures

Numerous countries across the globe have a national e-health initiative at some stage of investigation or implementation. This section focuses on a number of national e-health architectures, including those in Australia, Canada, UK, Germany, the Netherlands, and the USA.

2.2.1 Australia's national e-health strategy

Australia's national e-health approach adopts distributed Individual Electronic Health Record (IEHR) repositories which are expected to be developed across geographic regions, according to the strategic directions specified in the Australian Government's National E-Health Strategy [3]. An IEHR repository contains summarised patient health information which aggregates the health records coming from the original health information into integrated records across multiple locations. Australia's national e-health strategy also acknowledges that a central indexing or addressing mechanism is needed to link related health records which may reside in one or more locations. Australia's national e-health strategy for the distributed IEHR plan appears to follow a similar approach to Canada's e-health record architecture (see Section 2.2.2).

NEHTA was established to accelerate the adoption and progression of e-health in Australia in 2005. In particular, NEHTA [21] is mandated to deliver fundamental e-health services such as Healthcare Identifiers (HI), secure messaging and authentication, and a clinical terminology and information service. NEHTA released Connectivity Architecture V1.0 [22] for Australia's national e-health plan in 2008 and reissued Connectivity Architecture V1.1 [23] in June 2010. After comparing these two versions, it is apparent that no change has been made to the overall connectivity architecture in Version 1.1,

while there is a terminology change from Service Instance Locator (SIL) in Version 1.0 to Endpoint Location Service (ELS) in Version 1.1.

From a high-level perspective, NEHTA's Connectivity Architecture [22] comprises: (a) use of services; (b) national infrastructure services; and (c) interactions. In particular, the national infrastructure services within NEHTA's architecture include:

- Unique Healthcare Identifiers, including the Individual Healthcare Identifier (IHI) service for identifying patients, the Healthcare Provider Identifier – Organisation (HPI-O) service for identifying healthcare organisations, and the Healthcare Provider Identifier – Individual (HPI-I) service for identifying healthcare professionals;
- The National Authentication Service for Health (NASH), providing authentication services based on Public Key Infrastructure (PKI) in support of authentication, digital signing, and encryption for secure messaging; and
- An Endpoint Location Service (ELS), providing indexing services containing reference information to indicate the distributed locations of the source systems holding the related health records.

NEHTA [22, 23] appears not to have reached a conclusion regarding whether to choose a centralised, decentralised, or hybrid deployment model for the ELS. The centralised model is a central nationwide ELS system. The decentralised ELS model is implemented by each participating healthcare provider entity. Under a hybrid model, ELS services are hosted by a group of healthcare providers to serve self-service.

Chapter 7 confirms the relevance of the OTHIS/HINS goal and proposes "A Secure Architecture for Australia's Index Based E-health Environment" to support secure communications between healthcare providers and the Index System. The proposed architecture is based on the broad architecture of the Australian Government's National E-health Strategy [3] and NEHTA's Connectivity Architecture [22, 23]. This security architecture involves two

significant structures: i) the Index System; and ii) the Healthcare Interface Processor.

- The Index System is a centralised facility run at a national level as part of national infrastructure services. It is envisioned that the directory service will be devised in the context of a Domain Name Service (DNS), which uses a hierarchical distributed database architecture. To maximise the efficiency of the indexing services, the Index System performs only fundamental services such as identification, authentication, and directory services, rather than providing network connectivity, messaging translation, addressing, routing, and logging services. The load of the national Index System should be relatively lightweight to undertake e-health indexing services efficiently to mitigate against the Index System explosion and traffic bottleneck risks. Such an approach is favourable in a geographically large country such as Australia.
- An appropriate high-trust interface module - a "Healthcare Interface Processor (HIP)" should be developed and deployed as the application proxy implemented at the healthcare provider entity's site to connect to the national Index System and other healthcare service providers. The design rationale underlying HIP is to provide a secured communication channel for an untrusted health information system connected to the Index System and for health information exchange among healthcare providers.

The security architecture of the Index System proposed in Chapter 7 draws on important lessons from the Internet's Domain Name System (DNS) for the development and deployment of the national healthcare Index System. This thesis embraces the hierarchical and distributed nature of DNS and defines the required components for a secure architecture for Australia's national e-health scheme. The DNS structure, determined (some) 25 years ago, is based around a globally distributed, hierarchical database architecture that relies upon replication for resilience and caching for performance. This research argues that the hierarchical nature of the DNS structure appears

suitable given that the Australian system must cater for a federated national structure with roles for the various State-level participants.

This thesis proposes the Healthcare Interface Processor (HIP) structure in Chapter 7, which enunciates the design principles and security provisioning of HIP. That is, the design philosophy of HIP draws on principles used in the Interface Message Processor (IMP)[1] of the Advanced Research Projects Agency Network (ARPANET). Each site uses an IMP to connect to the ARPANET network to isolate the potential hostile system connecting to the ARPANET network. It provides all necessary protocol conversion, network management, and security functions. For the same reason, the design rationale underlying HIP is to provide a secure communication channel for an untrusted health information system connected to the Index System and for health information exchange between healthcare providers. Wherever a connection to the national indexing system is required, a HIP facility has to exist. The design goal for HIP is to make it a "plug and operate" facility, which is easy and simple to use for healthcare providers, as well as having characteristics of high security, reliability, efficiency, and resilience. Such a design would be very beneficial and useful, particularly for healthcare providers. Further specific details of the HIP development and deployment are described in Chapter 7 of this thesis.

2.2.2 Canada's Electronic Health Record Solution (EHRS) Blueprint Infostructure

Canada's Electronic Health Record Solution (EHRS) Blueprint [24, 25] has been designed as a national e-health Electronic Health Record (EHR) architecture. Canada Health Infoway has been commissioned by the Canadian government to oversee the development and adoption of the Canadian national e-health framework. The federal EHR Infostructure comprises all subsets of jurisdictional EHR systems. Canada's EHRS Blueprint allows each jurisdiction to develop its own EHR system suited to its needs and jurisdictional legislative requirements based on the principles of the EHRS Blueprint.

[1] The IMP device was one component of the *early Internet*.

Canada mainly employs the integrated method of sharing electronic health records across multiple health information systems. Each jurisdictional EHR system consists of integrated and cross-referenced health data replicated from source data systems [24, 25]. Canada's EHRS Blueprint is a highly cross-referencing and index-based scheme linking relevant health records located at various registries and repositories.

Privacy and security requirements were not fully incorporated into Canada's EHRS Blueprint Version 1. The EHR Blueprint Version 2 incorporates privacy and security services into its conceptual architecture. These added services include identity protection and management, access control, user authentication, secure auditing, general security, consent directives management, encryption, and digital signatures [24].

The EHR Infostructure addresses privacy and security requirements by adopting the Canadian Standards Association Model Code and international standard ISO 17799 as codes of practice for information security management governance to safeguard electronic health data [26].

In order to achieve a high level of information assurance in health information systems, this thesis proposes a security-centric approach to OTHIS to address privacy and security requirements at each level of a modern health information system architecture to ensure protection when health data is at rest, being processed, and in transit.

In Canada's EHR Infostructure [24, 25], there is no direct communication between participating healthcare entities. Each participating healthcare entity interacts with the jurisdictional EHR system via a message broker called the Health Information Access Layer (HIAL) to upload and retrieve shared health data from the EHR Infostructure. When the HIAL receives a message update from a participating healthcare entity, it parses the message and updates the health records into the jurisdictional EHR system. When the HIAL receives a query message, it retrieves the requested health information from the EHR registries and repositories and then responds to the requesting entity. HIAL provides an interoperability platform including service

components, information models, and common messaging standards needed for the exchange of health data among disparate health information systems.

Interestingly, the design philosophy of the HIP facility proposed in Chapter 7 and the HIAL component in the Canadian EHR Infostructure [24, 25] both derive from the concept of the IMP developed by ARPANET. The IMP was responsible for providing all necessary protocol conversion, network management, and security functions. The HIAL element is part of Canada's EHR Infostructure, acting as a gateway to provide a collection of services between the EHR services and participating healthcare systems. The technology infrastructure of HIAL exists "in the cloud," and does not reside at the healthcare entity's end. This is in contrast to the HIP facility proposed in Chapter 7, which resides at each participating healthcare site to provide a secure communication channel for an untrusted health information system connected to the Index System. In addition, HIP acts as an interface/gateway for a healthcare provider's system to connect to other health information systems to exchange health information in a secure and reliable manner.

From this thesis perspective, Canada's EHR Blueprint [24, 25] appears to lay out a comprehensive national e-health architecture. The key challenge for this approach is the complexity of linking multiple jurisdictional EHR systems together to achieve interoperability. Additionally, this approach carries overwhelming integration costs for a full-scale implementation in a geographically large country like Canada.

2.2.3 National Health Service (NHS) in England

The UK National Programme for IT (NPfIT) [27], one of the largest public sector health IT projects in the world, was initiated in 2002 as a ten-year project to provide electronic health record management for 50 million patients in England. Its goal is to provide electronic health records, electronic booking of medical appointments, and electronic prescribing. NHS Connecting for Health is the agency of the UK Department of Health

responsible for delivering NPfIT in England. This unprecedented information technology project involves the significant investment of £12.4 billion over ten years, with the full cost of this project likely to range up to £20 billion. The project completion date was initially delayed until 2015; however, the completion date has since been further delayed to an unknown date. A criticism [28] has been that this project has been using inadequate safeguards to protect the privacy of patients. This programme is being implemented in England, while Wales is running another national programme. In general, the separate provisions of the United Kingdom's national e-health systems need to be made interoperable for information traversing national borders.

The NHS provides national e-health services in England on the "Spine." The Spine [29] is a nation-wide central database which stores summarised clinical information to improve healthcare quality and provide the convenience of accessible data. The functionalities of the Spine consist of identification and authentication, authorisation logic, directory services, routing, and clinical summary information. The major components of Spine architecture include:

- The Personal Demographics Service (PDS), which stores patient demographic information, such as unique patient identifiers, NHS Numbers, name, address, and date of birth;
- Spine Directory Services (SDS), which provides directory services for registered healthcare providers and organisations;
- National Care Record (NCR), which contains clinical information summaries extracted from local health information systems and source healthcare information locations;
- Legitimate Relationship Service (LRS), as an authorisation logic containing relationships between healthcare professionals and patients, and patient preferences on information accessing. LRS governs legitimate health providers with appropriate access privileges allowing access to patient record summaries; and

- Transaction Messaging Service (TMS), which provides routing services for the message requests and responses.

All clinical message flows from local health systems to the Spine are routed via the intermediary point, the TMS. The TMS subsystem routes the message from the requesting system to the NCR. If the requested clinical information is not sufficiently recorded in the clinical summary, the requesting entity needs to obtain the detailed health information located at the point of healthcare provision. The NCR subsystem obtains the required information from the source health system and then returns the information to the requesting system. When the TMS receives a clinical message update from the local health system, the TMS extracts the relevant information and updates the health information stored in the NCR [29]. There is no direct communication between participating health entities. The Spine architecture is considered a centralised management system. Meanwhile, the Spine also relies on indexing services to retrieve patient record details at the local level when required. Both the message gateways of Canada's HAIL and the UK's TMS exist "in the cloud." They play an integral role in connecting local health information systems to their national e-health infrastructure. The HIP facility proposed by this research exists at the local health system site connecting to the national e-health system.

2.2.4 German national e-health project

The German health Telematics project [30, 31] is implemented and managed by the government agency Gematik. This project introduces electronic healthcare cards and the necessary infrastructure to deploy national e-health services for more than 80 million patients. The project uses two types of electronic healthcare cards: i) Electronic Health Cards (EHC) for patients; and ii) Health Professional Cards (HPC) for medical professionals. This project is aimed at improving the efficiency and quality of healthcare and reducing healthcare service costs in Germany.

An Electronic Health Card (EHC), a smart card, contains a microprocessor to store patient personal data for administrative and medical purposes. A

patient can choose to store particular health information on his/her EHC, such as data used in emergency situations, drug interactions, and contraindication checks and references. Not only does an EHC contain administrative and clinical information, but it also provides basic security functions for authentication, integrity, and accountability services. The security provisions in the German Telematics program are also based on a PKI scheme to support authentication, digital signing, and encryption services [30-32].

It is argued [31] that the patient should be the owner of the patient data; therefore, patients should have the right to read, write, and delete their health information on their EHC. This raises concerns regarding the information integrity and data accuracy on EHC recorded by patients. Is such information appropriate and accurate for medical treatment? The German EHC application presents a feature of its national e-health strategy distinct from other national e-health initiatives. With this approach, the patient could carry his/her health data at all times like carrying a bank card; however, this forms a cumbersome and decentralised way of storing health information from an overall national e-health structure perspective.

The Health Professional Card (HPC) acts as an access token. Normally, it is used in conjunction with the patient's electronic health card to allow the health service provider to access the patient's health data. The HPC supports information security capabilities such as authentication, encryption, and digital signing for medical documents and electronic prescriptions. In emergency circumstances, a health professional is able to retrieve the patient medical data stored on the electronic health card directly even without accessing the Telematics platform [30-32]. This feature is realistic and viable only when the electronic health card is carried by the patient and the relevant health information has been stored on the EHC, noting that it is the patient's choice to store medical information on his/her electronic health card. The HPC has been designed specifically for e-health application, and should be considered differently to the more general smart card. Smart cards have an inadequate capacity (less than 150KB) to store comprehensive health information. Smart cards also have operational

constraints on temperature, humidity, and other environmental conditions. Hence, it may not be practical and reliable to store health information on a smart card.

The German Telematics architecture [30, 32], based on the standard ISO/IEC 10746-3: Information technology - Reference Mode: Open Distributed Processing (RM-ODP) model, comprises:

- A local health system connected to the national e-health platform (bIT4Health) for accessing central services of the Telematics infrastructure through a gateway interface called “bIT4Health Connector.” The connector, a hardware-based facility or integrated software with an information system, is installed at the local health system site to enable semantic interoperability and to provide data security services;
- The central Telematics platform, which provides three subsystems: i) Generic Common Services; ii) Common Services; and iii) Security Services. The Security Services subsystem is needed to access shared health data, such as authentication, authorisation, the signature timestamp, and access logging; and
- The backend system, which provides a set of resource providers that manages accessible data stores and external services.

The design principles of the bIT4Health Connector and the HIP facility proposed in this thesis share the following basic features:

- Both are installed at the local health system site; and
- Both act as a gateway/interface between the central service system and local health system for the provisioning of semantic interoperability.

A brief outline of the major differences between the bIT4Health Connector and the HIP facility follows:

- The HIP facility is aimed at building on the trusted platform to provide a resilient platform to carry out its tasks from Layers 1 to 7 of the seven-layer OSI model; and
- Not only does HIP envisage enabling semantic interoperability for healthcare information exchange, but it also provides critical security services, including presenting a trusted path to the national e-health infrastructure, mutual authentication, data protection, accountability, and operation flexibility with an emergency override function.

2.2.5 The Dutch national e-health strategy

The Dutch national basic e-health infrastructure ("AORTA") [33] has been constructed by the National IT Institute for Healthcare in the Netherlands (Dutch abbreviation: "NICTIZ").[2] The Dutch e-health implementation involves different components:

- The Citizen Service Number (Dutch abbreviation: "BSN");
- The Unique Healthcare Provider Identification (Dutch abbreviation: "UZI");
- The health information systems used by healthcare providers; and
- The National Healthcare Information Hub - National Switch Point (Dutch abbreviation: "LSP") to enable the exchange of healthcare information.

There is no clinical information stored at the national hub, LSP. The clinical data details and summaries reside at local health information systems and are not stored in a national database. The national e-health infrastructure provides standardisation of healthcare policy and the organisation of care processes and national infrastructural facilities to enable the sharing of electronic health information. The LSP includes services such as identification and authentication, authorisation, addressing, logging, and standardisation of messages services [34]. This style of sharing electronic

[2] NICTIZ is the Dutch national e-health coordination point and knowledge centre. More detailed information is available at http://www.nictiz.nl/, accessed 28/10/2010.

patient records across multiple health information systems is a model of an index-based scheme to access distributed electronic health information.

The LSP links healthcare providers' information systems together to enable the exchange of health information across the Netherlands. The Dutch national e-health network connectivity architecture requires the healthcare practitioners' health information system to be compliant with the "Qualified Health Information System (QHIS)" to enable it to connect to the LSP via Virtual Private Network (VPN) connections [33].

When the healthcare provider requests specific patient information which is located in other healthcare information systems, queries are relayed via the LSP. Namely, the healthcare service requester uses his/her UZI card to establish a connection between a QHIS and the LSP to query the health records of a given patient. The LSP then aggregates the requested health data from the health service providers and routes the health data to the requester. There is no direct communication between the healthcare service providing system and requesting system. The LSP also logs which healthcare providers have accessed patient data for accountability [34].

The Dutch national index system, LSP, is the central coordination point for health information exchange, containing authentication, authorisation, routing, and logging services. Such a scheme is an index-based scheme: participating health systems rely on indexing services to determine the locations of the relevant health records. Such an implementation model may appear suitable for a small-scale national e-health structure like the Netherlands. In a geographically large country, this implementation model will produce more network traffic, possibly creating performance bottlenecks. It is particularly prone to a single-point-of-failure weakness.

2.2.6 USA's Nationwide Health Information Network (NHIN)

The Office of the National Coordinator for Health Information Technology (ONC) of the U.S. Department of Health and Human Services is mandated to facilitate the development of the Nationwide Health Information Network (NHIN) [35]. The NHIN consists of many interconnected state, regional, and

local health information exchanges, structured in the manner of “network of networks”. In the U.S. national e-health context, a Health Information Exchange (HIE) is referred to as a HIE processor. The processor plays an important role in overseeing and facilitating the accessibility of health-related information exchange based upon agreed standards, protocols, and other criteria [36].

The USA’s National Institute for Standards and Technology (NIST) document titled “Draft Security Architecture Design Process for Health Information Exchanges (HIEs)” [37] provides guidance for the development of a security architecture for the exchange of health information. The HIE security architecture design process includes five layers to construct a technical security architecture for healthcare information exchange. The five layers consist of:

- Policies for overall legal requirements in protecting healthcare information exchange;
- Services for implementing policy requirements;
- Processes to define business requirement processes for enabling services;
- Definitions of technical constructs and relationships for implementing enabling processes; and
- Provisions for technical solutions and data standards for implementing the architecture.

The NHIN architecture [37] is based upon a hierarchical structure, which consists of a National Federation Health Information Exchange (HIE), Multi-Regional Federation HIEs, Regional HIEs, and ad hoc HIEs. The National Federation HIE has a national federated technical architecture, connects a number of Multi-Regional Federation HIEs, and involves multiple State jurisdictions. Multi-Regional Federation HIEs have a federated technical architecture and connect multiple regional HIEs. Regional HIEs are for small-scale and decentralised operations without State jurisdictional conflicts. These function as the “building blocks” for larger multiple regional and national HIEs. Regional HIEs can consist of two or more independent

healthcare organisations to share health-related information. The participating healthcare providers set up their own trust agreement to define security and privacy requirements for the exchange of health-related information. An ad hoc HIE model may occur when two healthcare organisations exchange health-related information based on mutual trust by traditional means, via telephone and fax.

Healthcare organisations can use CONNECT[3] to link health information systems to the NHIN for the exchange of health information. CONNECT, a joint adventure of 20 federal agencies, is developed as an open-source platform to connect to the NHIN. The key functions of CONNECT include authentication, provision of an authorisation policy engine, a patient record locator, and auditing. Certainly, making CONNECT a free and open-source platform to link health information systems to the NHIN can encourage greater participation in the exchange of healthcare information.

With the security architecture outlined by NIST [37], a healthcare entity can be authenticated via the Identity Federation Service or be redirected to the home organisation's authentication service to support single sign-on to access the HIE services. NIST determines that privilege access management is performed by service providers locally. The proposed architecture detailed in Chapter 7 of this thesis affirms that access authorisation is best performed where the resource system is located, as various healthcare organisations may have their own specific access requirements and processes.

The USA's NHIN is different from the Dutch and English national e-health architectures. In a large nation like the USA, a distributed and decentralised national e-health architecture appears suitable for scalability. USA's NHIN presents a high level of similarity to the context of the DNS hierarchical model. This type of approach can mitigate against the network traffic and performance bottleneck of the national e-health system.

[3] More information on CONNECT is available at http://www.connectopensource.org, accessed 21/09/2010.

2.3 Access control management in health information systems

Access control is one of the fundamental security mechanisms used to protect computer resources, in particular in multi-user and resource-sharing computer environments. "Access control" simply refers to a set of rules that specify which users can access what resources with which types of access restrictions. Various operating systems, network control systems, and database management systems (DBMS) can employ a choice of access control mechanisms to allow a user to access the protected resources of the system. It should be noted that in any information system a distinction may be made between "security aware applications" and "security ignorant applications." The latter applications usually depend solely upon access control facilities provided by an operating system, DBMS, and similar middleware. Implementing appropriate access control to data in any information system is a major security issue. Many instances of poor access control management practices leading to security and privacy violations are reported on a regular basis. Chapter 4 identifies and analyses information privacy violations or weaknesses which have been found in national infrastructure systems in Australia, the UK, and the USA, two of which involve departments of health and social services. The three identified scenarios all have a common security weakness issue directly related to access control management. Appropriate computer-based access control schemes can be deployed to address these information security issues.

The two traditional types of access control modes are Discretionary Access Control (DAC) and Mandatory Access Control (MAC). The Role-Based Access Control (RBAC) concept is complementary to both DAC and MAC techniques. RBAC enables easier management of access control by ensuring finer granularity in the access system.

2.3.1 Discretionary Access Control (DAC)

The DAC policy allows the owner of information to grant access permissions to other users or programs at his/her discretion without the system

administrator's knowledge. Each user has complete discretion over his/her own objects (such as records, files and programs). Thus, such a policy does not provide the actual owner of the system fully centralised access control over organisational resources. In fact, the system cannot identify the difference between a legitimate request to modify access control information which originated from the owner of the information and a request issued by a malicious program [38-41].

DAC mechanisms are fundamentally inadequate for strong system security. One of the major deficiencies with DAC is its vulnerability to some types of Trojan horse attacks. Trojan horses embedded in applications can exploit DAC's vulnerability to cause an illegal flow of information. Systems and applications that rely on DAC mechanisms are vulnerable to tampering and bypassing [40-44]. This shortcoming of DAC can be overcome by employing Mandatory Access Control (MAC) policies to prevent information flowing from higher to lower security levels.

The DAC mechanism is widely implemented for the purpose of managing access control by current commodity software such as Microsoft Corporation's Windows systems, and open-source systems such as Linux and the original Unix system. Increasingly, health information systems are being developed and deployed based upon commercial, commodity-level information and communications technology products and systems. In fact, the UK's National Audit Office [27] states that NHS information systems and healthcare applications are based on Microsoft information technology, which are DAC-based environments. Such general-purpose systems have been created over the last 25 years, often with only minimal security functionality and verification. In particular, access control, a vital security function in any operating system that forms the basis for application packages, has been founded upon earlier designs based on DAC. DAC systems were defined around an environment where data and program resources were developed and deployed within a single enterprise, which assumed implicit trust amongst users. This environmental model is no longer valid for modern health information systems.

Malicious or flawed applications can easily cause security violations in a DAC-based system. The existing computer-based access control mechanisms, particularly the DAC-based system, are not suitable or sustainable to safeguard the security of sensitive health information in a health information system. In contrast, trusted operating systems give high priority to privacy and security features; therefore, trusted health information systems are definitely the way forward. This thesis argues that health information systems should be developed and operated upon trusted operating systems so that health applications can exploit the inherent privacy and security features in the underlying operating systems. This research proposes a viable and sustainable access control management strategy for the protection of sensitive health data, in Chapters 4 and 6.

2.3.2 Mandatory Access Control (MAC)

Gasser [40] states that Mandatory Access Control (MAC) can be used to prevent certain/several types of Trojan horse attacks by imposing severe access restrictions that cannot be bypassed intentionally or accidentally. MAC can provide the ability to limit access to only legitimate users. The originators of the RBAC model, Ferraiolo et al. [39], underscore that MAC is necessary when truly secure system provisioning is required.

With MAC, each user possesses a clearance that is used by the system to determine whether a user can access a particular file. Access permissions are determined by a user's clearance compared with the sensitivity (or security) or classification level label on information stored in the system, not upon the user's discretion. The classification may contain an arbitrary number of categories; for example, a conventional hierarchical category set used in military environments might include "top secret," "secret," "confidential," and "unclassified." Each user possesses a clearance that is used by the system to determine whether a user can access a particular file. The access permission to information is determined by the user's clearance compared to the security level of information stored in the system. This is also known as a multi-level security (MLS) policy, which was first introduced by Bell and LaPadula (BLP) [45] in the 1970s.

With the MLS policy, BLP propose an access control system in the form of a mathematical model for defining and evaluating computer security. This model is designed to address the enforcement of information confidentiality aimed at the prevention of unauthorised information leakage. The BLP model defines two basic rules for making access control decisions: i) the Simple property; and ii) the Star property. The Simple property regulates whether a subject is allowed to read an object (i.e., if the subject's clearance level dominates the security level of the object). It is also known as the "no read up" policy. The Star property determines whether a subject is allowed to write to an object (i.e., if the security level of the object dominates the subject's security clearance level). This is referred to as the "no write down" policy [39, 40]. The traditional MAC policy was originally designed for a military environment based on the MLS hierarchical structure and was quite rigid in its application.

2.3.3 Role-Based Access Control (RBAC)

Role-Based Access Control (RBAC) is based upon the role concept in managing access control where access permissions are associated with roles. Users are assigned to appropriate roles within the organisation. The user must be assigned as a member of a role in order to perform an operation on an object. Ferraiolo et al. [39] state that the driving force behind the RBAC model is to simplify the management of authorisation. Assigning users' access permissions to each protected object in the system on an individual user basis, particularly in large-scale enterprise systems, is an onerous process in security management. With RBAC, users are granted membership into roles according to their responsibilities and competencies. User membership of roles can be added and revoked easily. Updates of assigning privileges can be achieved through role assignment rather than updating permission assignments for individual users. RBAC supports users' access rights based on such parameters as job function, enforcement of least privilege for administrators and users, enforcement of static/dynamic separation of duties (SOD), and hierarchical definitions of roles.

There is extensive literature [1, 7, 12, 46-50] related to the use of the RBAC mechanism for authorisation management in health information systems, because role models are suitable for the representation of roles in hospital settings. Despite several advanced RBAC features, RBAC also brings a number of limitations. Significantly, Linden et al. [1] and Reid et al. [49] contend that RBAC does not efficiently support practical policies to grant or deny access to a particular person. In addition, RBAC management becomes complex when the number of resources and roles increases. An implementation of an RBAC model can provide the ability to reflect the organisational policy under an internal organisational structure; however, it is complex to apply an RBAC model to an inter-organisational structure [1]. To date, there is still a lack of available products to support the full features of RBAC. Ferraiolo et al. [39], the developers of the first model for RBAC and proposers of the RBAC standard, state that RBAC is policy-independent and policy neutral in not enforcing any particular protection policy. Ferraiolo et al. [39] also point out that the availability of RBAC does not obviate the need for MAC and DAC policies. MAC is particularly needed when confidentiality and information flow are primary concerns.

2.3.4 Rethinking access control models in health information systems

Current moves toward Web-based identity and authentication structures present a major challenge where such structures are not based on highly trusted operating systems. All applications and supporting software which necessarily reside atop the untrusted operating systems are also untrusted. Building on experience with DAC and MAC structures, this research argues that the need for a radical re-think is absolutely crucial in the understanding of access control in light of modern information system structures, legislative and regulatory requirements, and security operational demands in health information systems.

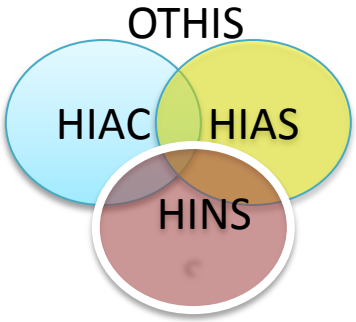
More recent research has modernised the traditional MAC approach to a flexible form of MAC (Flexible MAC) [51, 52] to overcome traditional MAC limitations. The U.S. National Security Agency designed and engineered

Security Enhanced Linux (SELinux) with a security architecture named the Flux Advanced Security Kernel (Flask) [52]. The Agency aims at setting an example of how Flexible MAC could be added to a mainstream operating system to greatly improve the security of the system. To date, the Flexible MAC architecture has been integrated into several other operating systems, including the Solaris operating system, the FreeBSD operating system, and the Darwin kernel. The Flexible MAC architecture provides a balance between security needs and flexibility of implementation that allows the security policy to be modified, customised, and extended as required in line with normal application and system requirements. The Flexible MAC architecture also provides separation of security domains as a fail-safe feature to enable the confinement of damage caused by the probability of malicious or flawed code execution [43]. The Flexible MAC architecture includes the separation of the security policy logic from the enforcement mechanism. This enables the independent policy module to be modified and extended as required without affecting the rest of the kernel or having the need to restart the system.

The OTHIS/HIAC presented in this thesis is a Flexible MAC-based model accompanied by RBAC properties to simplify authorisation management. This degree of simultaneous control, flexibility, and a refined level of granularity is not achievable with DAC, RBAC, or MAC individually. To determine the practical viability of an HIAC model for a health information system, a proof-of-concept prototype was built, based on an SELinux computer platform [53]. This work was carried out at the primitive stage of SELinux project development. As SELinux continues to advance and evolve, Chapter 6 presents the HIAC model with an updated proof-of-concept prototype. Preliminary results of this research indicate that the broad philosophy of Flexible MAC appears ideally suited to the protection of the healthcare information systems environment. The UK Cabinet Office [54] deploys SELinux as a secure platform to access the NHS's finance system.

2.4 Application security in health information systems

A modern health information system architecture would normally consist of health application services, middleware, a database management system (DBMS), a data network control system, and an operating system and hardware, as shown as in Table 1 (c).

<table>
<tr><td rowspan="2"></td><td colspan="2">Traditional models</td><td rowspan="2">(c) Modern health information system Architecture</td><td rowspan="2">(d) New proposed models – OTHIS</td></tr>
<tr><td>(a) OSI</td><td>(b) TCP/IP</td></tr>
<tr><td rowspan="8">Software System</td><td>Application</td><td rowspan="2">Application</td><td rowspan="2">Health application
Middleware
DBMS</td><td rowspan="3"> 
</td></tr>
<tr><td>Presentation</td></tr>
<tr><td>Session</td><td>(not present)</td><td rowspan="3">Data network management system

Operating system</td></tr>
<tr><td>Transport</td><td>Transport</td><td rowspan="2">Trusted operating system</td></tr>
<tr><td>Network</td><td>Internetwork</td></tr>
<tr><td>Data Link</td><td rowspan="2">Network Access</td><td>Trusted firmware</td></tr>
<tr><td>H/W</td><td>Physical</td><td>Hardware</td><td>Trusted hardware</td></tr>
</table>

Table 1: (a) OSI model, (b) TCP/IP model, (c) general health system architecture, and (d) OTHIS

Blobel et al. [47] argue that security application services should be placed at the core of security architecture design, as they consider application security deals with the trustworthiness of the behaviour of the application. Blobel et al. [55] consider that credentialing, privilege management, user management, role management, authorisation, role-base access, and audits are basic requirements of application security services. Weippl et al. [56] believe that security aspects for ubiquitous computing in healthcare contain application security, communication protocol security, and other related security services. Maji et al. [57] state that application security has gained much attention since the recent rise in security violations at the Web application level.

The overall aim of the OTHIS/HIAS model is to address the data protection requirements at the application level in health information systems. HIAS is located at the Application Layer and Presentation Layer of the Open Systems Interconnection (OSI) model and the Application Layer of the Transmission Control Protocol/Internet Protocol (TCP/IP) model to provide security features, as shown in Table 1. These security features are often required by a healthcare application at a data element level through to a service level. While privacy and security requirements directly relate to identifiable data and information, those health information system elements sitting at higher level information system layers cannot be ignored.

2.4.1 Healthcare application security on a Web Services platform

Web Services (WS) and Service-Oriented Architecture (SOA) concepts and implementations are proliferating. The security architecture outlined by the USA's National Institute Standards Technology (NIST) [37] uses WS technologies to construct HIE systems. Graauw [58] clearly sets the scene for the emergence of a WS-oriented implementation of next-generation health information systems. In Australia, NEHTA [59] also recommends using an SOA approach in the design of healthcare application systems and the use of WS as the technology standard for implementing secure messaging systems. NEHTA argues that development of information systems around WS technology is the direction in which the information and communications technology industry is heading. It is also accepted as best practice for the design of scalable distributed systems today. The SOA approach is claimed [59] to lead to more reusable, adaptable, and extensible systems over other techniques. NEHTA supports the concept that WS technology has gained notable attention within the information and communications technology industry and its use is extending in both popularity and market penetration. NEHTA addresses the security issue for secure messaging by defining a series of technical implementation examples [60-62] for XML Secured Payload with XML Encryption [63] and XML Signature [64]. NEHTA focuses on secure messaging and places security at the Transport Layer; however, it neglects to address privacy and security

requirements at each level within a modern health system architecture to ensure the complete protection of sensitive health data.

WS technology can incorporate security features in the Application Layer; for example, placing the label “WS-Security” in the header of a Simple Object Access Protocol (SOAP) XML message [65]. WS-Security provides a set of mechanisms to maintain finer granular levels of security services, such as authentication, confidentiality, integrity, and non-repudiation at an element level. For example, WS-Security defines how to use XML Encryption and XML Signature processes in the SOAP to secure message exchanges. WS-Security incorporates security features in the header of a SOAP message, which operates in the Application Layer. WS-Security by itself does not provide any guarantee of security for Web Services. In fact, it needs to rely on lower layers of security provisions for a complete security solution.

OTHIS/HIAS also addresses the situation where WS structures are being used as the major health informatics information transport methodology. OTHIS recognises that the SOA approach, implemented through a WS structure, has become a major information architecture paradigm. As such, any healthcare security architecture must be capable of handling the WS paradigm in a trusted, secure, and efficient manner. This provides end-to-end security for data and messages in transit, but depends upon an underlying trusted system to provide fundamental system security.

2.4.2 Health Level Seven (HL7) v3 standard

Health Level Seven (HL7) [66] is considered a form of Electronic Data Interchange (EDI) standard for the healthcare domain. HL7 standards are American National Standards Institute (ANSI)-accredited, and have been developed to enable interoperability to support the exchange of clinical, financial, and administrative data across heterogeneous platforms. HL7 standards are developed by Health Level Seven International, one of several ANSI-accredited standards-developing organisations working in the healthcare sector. The term ‘HL7’ makes reference to the Application Layer of the OSI model, which focuses on Application Layer protocols for

information exchanged between computer applications. Blobel and Holena [65] state that HL7 functions as a middleware layer for health information systems.

In developing a trusted system architecture for a health information system, it is important to understand the philosophy of HL7 as a clinical messaging standard to enable interoperability for the exchange of healthcare information. A number of countries have adopted the HL7 standard as the messaging protocol for health information exchange, including the USA, the UK, Germany, Canada, and Australia. NEHTA is responsible for setting the direction for electronic messaging standards in Australia's health sector. It has endorsed HL7 as Australia's national standard for the electronic exchange of health information [64].

There is a lack of security research development on the HL7 security concept and model. The HL7 security framework [67, 68] and standard guide for HL7 communication security [69] were developed in 1999. The HL7 protocol does not define security provisions, but depends upon the security functions provided at the Application, Transport, or Network Layers. This is also affirmed by Blobel et al. [69]:

> *Following the HL7 client/server network architecture using communication servers for end-to-end communication where applications meet and exchange their messages, the security services providing HL7 communication security MUST be placed on the Transport Layer or Application Layer of each principal.*

In recent years, Health Level Seven has released a number of ANSI approved security-related standards for HL7 v3 [70], including:

- HL7 Version 3 Standard: Role-based Access Control Healthcare Permission Catalog, Release 1 in 2008 [71]; and
- HL7 Version 3 Standard: Role-based Access Control Healthcare Permission Catalog, Release 2 in 2010 [72].

The HL7 Version 3 Standard: Transport Specification - Web Services Profile [73] adopts WS-Security to provide security services for HL7 messaging. In essence, this document is provided to illustrate the state of the art at the

current time and is not to be used for implementation. The HL7 payload is encapsulated in a SOAP envelope and then transported over Secure Hypertext Transfer Protocol (S-HTTP) via the Internet, with HL7 requiring the use of the WS-Security mechanisms to provide message-level security. The main limitation of HL7, however, rests in it requiring the lower layer of security and privacy structures to enable trust in an overall health information system and its interoperability. It should be noted that without a trusted foundation, the data security of any health applications will be vulnerable.

HIP aims to run on top of trusted hardware, firmware, and an operating system to provide a fundamental security base, as well as providing functions from Layers 1 to 7 of the OSI model. HIP is also capable of running WS-Security, as well as carrying out message mapping and conversion to enable healthcare information exchange among disparate health systems. The functional details of HIP are provided in Chapter 7.

2.4.3 Healthcare data protection for legal compliance

Legislation, regulation, and enterprise policy in relation to privacy and security in health informatics normally involves specific data entities (such as service provider and patient identity), rather than higher-level information technology constructs. Such data entities, however, must themselves exist within those same larger constructs (such as databases, messaging systems, operating system file structures and the like). While privacy and security requirements directly relate to identifiable data and information, those health information system elements sitting at higher level information system layers cannot be neglected.

The primary goal of the Security Rule of HIPAA is to protect the confidentiality, integrity, and availability of individually-protected health information. 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 electronic health data, including access control, audit, integrity, entity authentication, and transmission

security. The security standards defined in the Security Final Rule are intended to be technology-neutral. Covered entities (such as healthcare providers, health plans, and healthcare clearinghouses) have options in selecting the appropriate technology to protect electronic health information, based on the nature and resources of their business [19, 74].

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 HIPAA requirements.

In the case of Australia, the principal Federal statute is the *Privacy Act 1988* [75] which has provisions for the protection of the privacy of personal information including eleven Information Privacy Principles (IPPs). The Commonwealth and Australian Capital Territory (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 [76].

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* contain ten National Privacy Principles (NPPs). The NPPs apply to large private-sector organisations with an annual turnover of more than $AUD3 million, 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 [77].

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 [78] and s.95A [79] 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 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 s.95 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 s.95A applies to medical research that involves access to personal information held by organisations in the private sector.

Australian privacy laws and health-related privacy legislation prescribe no particular technology to protect personal information. For instance under the Information Privacy Principles (IPP) of the *Privacy Act 1988* (Principle 4 – Storage and security of personal information), Principle 4(a) requires an organisation to take reasonable steps to protect personal information. The National Privacy Principles (NPP) in the *Privacy Amendment (Private Sector) Act 2000* also require a record keeper to protect personal information by security safeguards as is reasonable. No specific security mechanisms are specified in both the IPP and NPP; thus, any reasonable and adequate security measures are allowed for protecting personal information.

The Australian Law Reform Commission (ALRC)[4] commenced a 28-month comprehensive review on the *Privacy Act 1988* in 2006 and released the final report in 2008 [80]. This sub-section addresses two of the ALRC's recommendations relating to privacy principles and handling health information. The ALRC recommends that the *Privacy Act* should harmonise the existing privacy principles IPP and NPP into a single set of Unified Privacy Principles (UPP), applicable to all federal government agencies and the private sector across Australia for national uniformity. The ALRC also recommends new privacy regulations should be developed separately in

[4] The role of the ALRC is to conduct inquiries and to make recommendations to the Australian Government so that it can make informed decisions about law reform.

controlling privacy of health information, including managing electronic health records and facilitating the use of health data for medical research.

The Australian Government addresses the ALRC's 295 recommendations in two stages. The first stage of response [81] was issued in 2009 to address 197 ALRC recommendations. The Government has agreed to streamline these two sets of privacy principles into the UPPs. It has, however, rejected the ALRC's recommendation to introduce separate health privacy regulations, as the Government believes that the substantive rights and obligations in handling health information and other personal information should be in the primary legislation. At the time of writing this thesis, the Australian Government still has to address the remaining 98 recommendations of the ARLC in its second stage of response.

This research will continue to observe the update of privacy and e-health privacy legislation in Australia, in order to design the OTHIS architecture for legal compliance. The overall aim of the OTHIS/HIAS model is to address the data protection requirements reflected in such regulatory instruments with the practical security services and mechanisms provided by healthcare application systems. In this regard, HIAS aims at defining privacy and security requirements at the Application Level in a health information system.

2.5 Communication security in health information systems

Normally modern health information system architectures are based around distributed network systems; thus, communication security services in health information systems play a central role in protecting sensitive health information in transit. In general, communication security services consist of network-level security services and mechanisms to authenticate claims of identity, to provide appropriate authorisations following authentication, to prevent unauthorised access to shared health data, to protect the network from attacks, and to provide secure communications for health data transmission over the associated data networks.

2.5.1 Common network security measures

There are numerous common security measures which can be seen as possible solutions in addressing the transmission security for healthcare-specific systems or non-healthcare-specific systems. For example, firewalls [82] may be used to enforce network security policies for enterprises to control traffic between internal and external networks, as well as to reduce internal network exposure. Virtual Private Networks (VPN) [83] can be used for point-to-point security for protecting data privacy over a public network through the use of cryptography. Digital signing and encryption mechanisms can and should be used to achieve data confidentiality and integrity in transit for end-to-end security against forgery, repudiation, or eavesdropping. Intrusion Detection Systems (IDS) [84] can be used to monitor network and system activities to identify malicious activities or security policy violations and to produce reports to notify security administrators, as appropriate. To enforce accountability, audit trailing can be used to record any security-relevant events that may occur within the information system whenever deemed appropriate. The following two sections focus on identification and authentication services for health, as well as network communication connectivity mechanisms used to link to the national e-health infrastructure.

2.5.2 Identification and authentication services in healthcare

The national Healthcare Identifiers (HI) Service is demonstrated to be one of the building blocks for the national e-health infrastructure. The national HI scheme for identification services must be deployed prior to the implementation of the national e-health system. The HI Service can enable accurate identification of individuals and healthcare providers in the national e-health environment. Australia's National Authentication Service for Health (NASH) [85] is being designed by NEHTA to provide authentication, digital signing, and encryption services based on a PKI scheme. For the authentication function, NASH will issue digital certificates and tokens to registered and certified healthcare providers and organisations to enable access to the HI Service when implemented.

A number of research papers [6, 8, 9, 12, 50, 86-90] have been written to discuss the adoption of PKI as a means for supporting authentication and digital signing services for healthcare systems. For example, the German health Telematics project is using smart cards based on a PKI scheme to support authentication and digital signing services, as stated in Section 2.2.4. Similarly, the European TrustHealth project [9] uses Health Professional Cards (HPC) as the main authentication token and digital signing based on a PKI scheme for cross-border communications.

Takeda et al. [89] report a community-based health information system in Osaka, Japan, is also based on a PKI system to support authentication, digital signing, and other security services for the exchange of health information. Takeda et al. discuss a number of limitations to deploying PKI in that regional health information system, including PKI operation and management costs, PKI compatibility problems, and medical document retention issues.

Numerous e-government, e-health, and e-commerce schemes have reflected commonly a uniform belief in the advantage of certificate-based PKI to support authentication, digital signing, and encryption services, irrespective of a number of PKI limitations. These limitations include high operation and management costs and performance, interoperability, and scalability problems. Only a few [6, 89] have acknowledged and discussed shortcomings of PKI deployment that impedes the successful deployment of PKI in a large-scale environment. While this thesis does not specifically examine the detailed PKI system structures, PKI's influence on the overall health information system architecture cannot be ignored.

2.5.3 Network communication gateway connecting to national e-health infrastructure

A number of countries adopt a network communication gateway to link health information systems to their national e-health infrastructures. A network communication gateway can play a central role as a proxy server, interface/connector, broker, or hub to provide necessary message

conversion, to enable semantic interoperability, and/or to coordinate message queries and replies. It can also provide security functions via authentication, an authorisation policy engine, a health data record locator, and auditing services. Table 2 summarises the functions of network communication gateways from five exemplary countries; namely, Canada, England, Germany, the Netherlands, and the USA, as described in Section 2.2.

	National e-health program	Communication gateway	Function
Canada	Electronic Health Record Solution (EHRS) Blueprint	Health Information Access Layer (HIAL)	• To provide a standardised platform for health information systems connecting to EHRS Infostructure • To provide an interoperability platform for the exchange of EHR data
England	Spine	Transaction Messaging Service (TMS)	• To provide message transfer coordination for routing health data requests and responses
Germany	better Information Technology for Health (bIT4Helath)	bIT4Health Connector	• To provide a consistent platform connecting to bIT4Health infrastructure for enabling semantic interoperability
The Netherlands	AORTA	National Switch Point (LSP)	• To provide identification and authentication, authorisation, addressing, routing, logging, and standardisation of messages services
USA	Nationwide Health Information Network (NHIN)	CONNECT	• To provide an open-source platform linking health information systems to the NHIN • To provide authentication, an authorisation policy engine, patient record locator and auditing services

Table 2: Exemplary Network Communication Gateways

While coordination of data exchange must play a vital role in any national electronic health record scheme, the overall information assurance of the system cannot be left to the associated messaging system alone. For example, Graauw [58] emphasises that, *"... all messages are exchanged between a provider HIS and a healthcare information broker (HIB), which in turn may send the data contained in those messages to other healthcare parties."* The importance of the assurance of all intermediary computer systems cannot be underestimated, as these may quickly become the "weakest link." Graauw clearly acknowledges that, *"It is possible to build a*

reliable and secure framework for sending medical data over the Internet … provided all transport nodes are reliable." This provision appears to be noted in much of the research conducted to date, based around the assured transportation of electronic medical records. This places great emphasis again on the need for high-trust computer systems to act as intermediary nodes at all points in the network, and particularly at any integration or brokerage points.

The HIP proposal of this thesis acts as an application proxy implemented at the healthcare provider's site to connect to the national e-health infrastructure, as well as to communicate with other health information systems. Distinctively, the design rationale of the HIP proposal is to provide a secure communication channel for an untrusted health information system connected to the national e-health system and for health information exchange between healthcare providers. In particular, the technical design of the HIP proposal contains its own on-board crypto-processor based on a trusted computing-based module to store cryptographic keys. HIP, a self-contained unit configured with an IP address, is capable of running Web Services. HIP carries out its works at all layers of the seven-layer OSI model. As mentioned in Chapter 1, it is envisaged that HIP achieves provisions of security services and mechanisms based upon the security and management concepts of OSI IS7498-2 [91], including:

- To establish a trusted path to connect to the authorised indexing system;
- To provide a mutual authentication function between healthcare providers and the national e-health system;
- To facilitate secure healthcare information exchange in transit;
- To provide data protection with appropriate access control mechanisms;
- To provide semantic interoperability to enable healthcare information exchange between disparate healthcare systems with varying security mechanisms;

- To support accountability when healthcare information has been accessed; and
- To provide operation flexibility with “emergency override” and capacity flexibility for various scales of healthcare organisations.

Further specific details of the HIP provisions are described in Chapter 7 of this thesis.

2.6 Standards and specifications

The purpose of standardisation is to enable a consistent baseline for reusability, interoperability, and scalability. Carroll [92] states, “*Standards are an essential part of modern software ecosystems. Without standard HTML, standard TCP/IP or standard HTTP, a global Internet would not exist.*” In fact, there are innumerable standards related to health informatics on both national and international bases. Note that this section does not intend to provide an exhaustive list or overview of health informatics standards, as that is impractical. This section does, however, aim at identifying those standards which may contain sections relevant to the subject of this thesis.

2.6.1 OSI 7498-1, OSI 7498-2 and TCP/IP

The OSI 7498 is a well-known reference model used as a baseline for the categorisation of network communication functions and assessment. OSI 7498 is divided into four parts. This research is related to the first two parts:

- ISO/IEC 7498-1:1994 Information Technology – Open Systems Interconnection – Basic Reference Model: The Basic Model [93]; and
- ISO 7498-2:1989 Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture [91].

The OSI seven-layer model is well known and acknowledged as a base for categorisation of cross-computer platform services, as shown in Table 1(a). The top two layers, Layer 6: the Presentation Layer, and Layer 7: the

Application Layer, would appear to play a major role if more fine-grained levels of control are required, particularly in relation to health information systems based around distributed computer systems. For example, under OSI it was accepted that Layer 6 would provide the following services to an application sitting above it in Layer 7:

- Data formatting – including translation between different character and even computer "word" coding schemes, such as American National Standard Code for Information Interchange (ASCII), *Extended Binary Coded Decimal Interchange Code* (*EBCDIC*), Unicode, "little-end" vs. "big-end" addressing, etc.; encryption and decryption services at an appropriate level of granularity ("selective field encryption");
- Provision of any compatibility requirements for the operating systems on the computers connected via the OSI scheme; and
- Encapsulation of application-level data into appropriate blocks needed for transmission.

In general, the OSI's seven-layer model can be further subdivided into two groups, including:

- Software-oriented services are related Layers 5, 6 and 7; and
- Data/network communication functions are related to Layers 1 to 4.

It is appropriate to place middleware into Layer 6 of the OSI model, closely associated with the Application Layer. The security of middleware itself fits into Layers 5 and 6. Under the OSI model, Layers 5, 6 and 7 were traditionally deemed to be part of a computer-based information system. Layers 1 to 4 are related to management controls at the Network Layer. With the OSI model, the layer above calls on the layer below for security services and mechanisms.

In reality, a fully operational system based on the seven-layer OSI model has never attained strong market acceptance. The OSI model envisaged management and control facilities existing at each layer, but many of the

detailed specifications and activities at each layer were never completed. Instead, TCP/IP (Table 1 (b)) is the model used globally for large-scale structures in network communications. Table 1 (a) and (b) present a comparison of the OSI and TCP/IP layering models. It is worth noting that the OSI seven-layer model clearly identified Session and Presentation layers, whereas these are not present in the TCP/IP model. Indeed, these two layers appear to be totally immersed in the overall Application Layer. The TCP/IP model does not match the OSI model exactly (Table 1 (a)); however, the processes defined in the OSI model are contained in the TCP/IP layers.

It should be noted that throughout this thesis, the seven layers of the OSI model have formed an overall template for the categorisation and classification of distributed systems technology. Nevertheless, with the acceptance of the TCP/IP model as the dominant global network structure through the Internet, the OSI classification techniques used in this thesis must be viewed in light of this reality. In fact, the security architecture proposed under the OSI 7498-2 (Basic Reference Model - Part 2: Security Architecture) [91] remains, in principle, valid when considering overall security architectures in such environments as health information systems.

Normally, health information systems are based around distributed network systems; therefore, it is entirely appropriate to relate the general health information system architecture to the OSI model as well as the TCP/IP model. This research relates and describes the roles and functions performed by each module of the OTHIS architecture, and how they fit into the layers of the OSI 7498-1 model [93] and TCP/IP model as well as ISO 7498-2 [91] (Table 3) security services and mechanisms in a healthcare environment.

Mechanism / Service	Encryption	Digital Signature	Access Control	Data Integrity	Authenti-cation Exchange	Traffic Padding	Routing Control	Notarisa-tion
Peer Entity Authentication	Y	Y	*	*	Y	*	*	*
Data Origin Authentication	Y	Y	*	*	*	*	*	*
Access Control Service	*	*	Y	*	*	*	*	*
Connection Confidentiality	Y	*	*	*	*	*	Y	*
Connectionless Confidentiality	Y	*	*	*	*	*	Y	*
Selective Field Confidentiality	Y	*	*	*	*	*	*	*
Traffic Flow Confidentiality	Y	*	*	*	*	Y	Y	*
Connection Integrity with Recovery	Y	*	*	Y	*	*	*	*
Connection Integrity without Recovery	Y	*	*	Y	*	*	*	*
Selective Field Connection Integrity	Y	*	*	Y	*	*	*	*
Connectionless Integrity	Y	Y	*	Y	*	*	*	*
Selective Field Connectionless Integrity	Y	Y	*	Y	*	*	*	*
Non-repudiation, Origin	*	Y	*	Y	*	*	*	Y
Non-repudiation, Delivery	*	Y	*	Y	*	*	*	Y

Legend: "Y" = Yes. It means the mechanism is considered to be appropriate, either on its own or in combination with other mechanisms.
* refers to the mechanism is considered not to be appropriate

Table 3: OSI 7498-2 security services and mechanisms

While Table 3 clearly identifies the relationship between security services and their underlying mechanisms, this level of detail is normally provided in the software systems which are part of an overall information system security architecture. In a broad sense, the OTHIS architecture intends to encompass those security services and security mechanisms described in Table 3.

2.6.2 ISO 27799 Health informatics -- Information security management in health using ISO/IEC 27002

ISO 27799 [94] provides a set of guidelines to health organisations and other custodians of health information to support the interpretation and implementation in maintaining the confidentiality, integrity and availability of

health information via the implementation of ISO17799[5] and ISO 27002.[6] ISO 27799 applied to health information covers all forms of health information, all types of storage media, and all means of transmission.

ISO 27799 specifies an information security management system for the health sector. This thesis has not developed the structures and procedures pertaining to information security management systems, since this research is related to a security architecture design for health information systems. In general, the security control provisioning of OTHIS sustains the information security management described in ISO 27799.

2.6.3 CEN 13606 Health information – Electronic health record communication

CEN13606 Health informatics - Electronic health record communication, is a European standard series prepared by CEN (European Committee for Standardisation)/TC (Technical Committee) 251,[7] which has been submitted to ISO Technical Committee (TC) 215[8] as a technical standard series ISO 13606, in addition to being adopted as an Australian and British standard series. The CEN13606 standard series consists of five parts [95-99], which define logical models and interfaces needed in supporting the generic electronic health record communication and archetypes between disparate electronic health systems.

This research relates to Part 4: Security of CEN 13606, which describes a mechanism for specifying the privileges necessary to access EHR data. In particular, Clause 6.1 Record Component Sensitivity of CEN 13606 Part 4 [95] classifies sensitivity levels of a health record into:

[5] ISO 17799 is widely adopted to provide best-practice guidance for information security management controls around the world.
[6] ISO 27002 is titled “Information Technology Security Techniques – Code of Practice for information security management,” which is related to the ISO 27000 family series in relation to the information security management topics.
[7] CEN/TC 251 is the Technical Committee of the European Committee for Standardisation working on the standardisation of health information to enable compatibility and interoperability.
[8] ISO TC 215 is the ISO Technical Committee working on the standardisation of health information to enable compatibility and interoperability between independent health information systems.

- Sensitivity Level 1: Care management;
- Sensitivity Level 2: Clinical management;
- Sensitivity Level 3: Clinical care;
- Sensitivity Level 4: Privileged care; and
- Sensitivity Level 5: Personal care.

Level 1 has the least degree of sensitivity and Level 5 indicates the highest sensitivity level of a health record.

It appears that NEHTA [2] partially adopts this sensitivity labelling classification mechanism with only two levels: “Clinical Care” and “Privileged Care.” NEHTA defines the “Clinical Care” label as normally referring to clinical information that may be accessed by all healthcare providers involved in the patient’s healthcare. Health data labelled as “Privilege Care” can only be accessed by healthcare providers who have been nominated by the patient. This is a coarse granularity for consent. It may not be sufficient to meet the situation where information access needs to be performed at a finer granularity. Chapter 8 of this thesis extends the sensitivity label mechanism outlined by NEHTA with “inclusive access” and “exclusive access” provisions to support a finer level of granularity for patient consent.

2.6.4 ISO/TS 18308 – 2005 Health informatics – Requirements for an electronic health record architecture

The purpose of ISO/TS 18308 is to assemble and collate a set of clinical and technical requirements for an electronic health record architecture that supports using, sharing, and exchanging electronic health records across different health sectors, different countries, and different models of healthcare delivery. This standard contains only one page (approximately 350 words) of generalised statements in relation to privacy and security requirements for an electronic health record architecture. These requirements are expressed in general terms, and those same terms form, with others, a basic set of requirements for the OTHIS structure.

2.6.5 HL7 v3

HL7 v3 standard has been described in Section 2.4.2.

2.6.6 openEHR Architecture

The openEHR Architecture [100] is developed by the *open*EHR Foundation.[9] This architecture intends to specify a set of standardised requirements to facilitate sharing health records across disparate health information systems, including requirements, abstract specifications, implementation technology specifications, computable expressions, and conformance criteria. The openEHR Architecture sees itself as a highly generic architecture to provide standards and archetypes for EHR architecture design.

The openEHR Architecture [100] contains a set of security and confidentiality requirements for EHR architecture design. It clearly states that, "*the openEHR specifications and core component implementation do not explicitly define any concrete mechanisms since there is great variability in the requirements of different sites.*" In fact, the main security measures directly specified by the openEHR only cover integrity and non-repudiation provisioning with access control, digital signature and audit trail mechanisms, however, there is no mention of other crucial security provisioning such as the confidentiality of health records. The openEHR architecture also openly states that, "*the openEHR HER imposes only a minimal security policy profile which could be regarded as necessary, but generally not sufficient for a deployed system (i.e. other aspects would still need to be implemented in layers whose semantics are not defined in openEHR).*" It seems that the security and confidentiality requirements in openEHR are still in their early stage of development. It is also not appropriate to use openEHR as the evaluation criteria for EHR architecture design.

[9] The *open*EHR Foundation is a non-profit independent community aiming to facilitate open-source and standardised implementations for sharing health records.

2.6.7 NIST's standard guide

One of the NIST special publications SP 800-66 is titled "An Introductory Resource Guide for Implementing the Health Insurance Portability Accountability Act (HIPAA) Security Rule" [101]. This publication discusses security considerations and provides a resource guide to assist conformance with the HIPAA Security Rule. Particularly, this resource guide provides guidelines for the implementations of the technical safeguards specified in the HIPAA Security Rule, including access control, audit control, integrity, authentication, and transmission security. This thesis meets all the requirements of the technical safeguards mentioned above in the OTHIS architecture. Specifically, OTHIS/HIAC is designed to address access control management for health information systems from the network, operating system, and database management system, up to the Application Level. One of the access control management activities in SP 800-66 addresses implementing the mandatory requirement to "establish an emergency access procedure." OTHIS/HIAC readily caters for this requirement by providing the flexibility of having an emergency override function by switching to a defined emergency policy in emergency circumstances and activating vigorous audit trail functions. In addition, OTHIS ensures that all information prior to transmission is digitally signed and encrypted for confidentiality, authentication, and message integrity.

2.6.8 NEHTA's standards and specifications

Part of NEHTA's mandate is to set standards and specifications to accelerate Australia's e-health adoption. As described in Section 2.2.1, NEHTA issued a number of publications on conceptual architecture for Australia's national e-health:

- Connectivity Architecture Version 1.0 (in 2009) [22];
- Connectivity: Implementation Guide Version 1.0 (in 2008) [102];
- Connectivity Architecture V1.1(in 2010) [23];
- Connectivity: Introductory Guide Version 1.1(in 2010) [103]; and
- Connectivity: Implementation Guide Version 1.1(in 2010) [104]; and

- NEHTA Strategic Plan 2009/10 to 2011/12 (in 2009) [21].

Chapter 7 of this research proposes a security architecture based around the Australian Government's National E-Health Strategy Summary [3], NEHTA's Connectivity Architecture and Guide [22, 102], and NEHTA's Strategic Plan 2009/10 to 2011/12 [21].

NEHTA has also developed a list of specifications and standards for secure healthcare messaging. Healthcare messaging software systems need to comply with NEHTA's technical specifications to develop healthcare messaging products and services. In 2010, a number of NEHTA's security message specifications have been adopted by Standards Australia,[10] including:

- ATS 5820:2010 E-health Web Services Profiles [105];
- ATS 5821-2010 E-health XML Secure Payload Profiles [106];
- ATS 5822:2010 E-health Secure Message Delivery [107]; and
- TR 5823-2010 Endpoint Location Service [108].

The Index System in the proposed security architecture (Chapter 7) is partially based on NEHTA's Service Instance Locator [109], which is the predecessor of TR 5823-2010 Endpoint Location Services [108].

2.6.9 OASIS and W3C standards

The Organization for the Advancement of Structured Information Standards (OASIS) is a standards body involved in developing Web Services standards to support interoperability. Recently, OASIS released a set of healthcare-specific WS standards, including:

- Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of XACML v2.0 for Healthcare Version 1.0 [110]; and

[10] Standards Australia is the Australian standards body recognised by the Australian Government.

- Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of Security Assertion Markup Language (SAML) for Healthcare Version 1.0 [111] .

The main purpose of these two profiles is to support authorisation decision requests and authorisation assertion expressions across enterprise boundaries. A healthcare service-requesting entity may send a request containing SAML assertions to carry authorisation attributes based on the SAML profile [111] for service invocation. The healthcare service-providing entity can parse and evaluate the assertions against its security and privacy policy and make and enforce an access decision based on the XACML profile [110]. The prototype developed in this research is not based on the XACML and SAML specifications owing to the inflexibility of the XACML and SAML descriptions for functional support, such as, multiple actions cannot be described in one XACML request and be transferred into the final authorisation decision statement. It is far more flexible to use any language specifications to describe security policies and to evaluate authorisation assertions and then to format the outcome with Web Services Description Language (WSDL) [112] and SOAP specifications [113].

Chapter 8 of this thesis develops a prototype to evaluate the practicality of the proposed security architecture in an index-based environment. This prototype generates and implements healthcare applications on a Web Services platform consistent with WSDL [112] and SOAP specifications [113]. In the test environment, the health information system implements service provision and invocation in WSDL through the support of Web Service interfaces for interoperability. WSDL and SOAP are developed by the World Wide Web Consortium (W3C), one of the standards bodies involved in defining architectures and the core technologies for the World Wide Web. WSDL specifies a standard way to describe the interfaces of a Web Service at a syntactic level and how to invoke network services in XML format. SOAP is an XML-based communications protocol to enable applications to exchange information via HTTP.

2.7 Instruments used in EHR systems

This section illustrates instruments used for electronic health record systems, including healthcare smart cards, and EHR repositories such as Microsoft Health Vault and Google Health.

2.7.1 Healthcare smart cards

Increasingly, smart card applications have been widely accepted and extensively used in a number of European countries for identification, authentication, and other related healthcare services, including the UK, Germany, France, Italy, Spain, Finland, Denmark, Sweden, and Belgium [114, 115]. For example, the German e-health project employs Electronic Health Cards (EHC) to store the patient's health insurance status and key clinical information, and Electronic Professional Cards (HPC) for healthcare professionals for verification, digital signing and encryption functions, as described in Section 2.2.4. According to the Frost and Sullivan Market Insight [114] issued in 2010, France has been one of the earliest European countries to introduce healthcare smart card applications in the late nineties. In the UK, the NPfIT programme also uses smart cards to carry patient data, electronic prescriptions, and medical appointment booking information. In the case of the Scandinavian countries Finland, Norway, and Denmark, their national health systems use healthcare smart cards to enable access to public healthcare services with concession rates or complimentary healthcare services. A number of European countries combine healthcare cards, social security cards, and/or health insurance cards, as in Spain, Belgium, and Luxembourg. This is for identification and authentication provisioning, as well as the storage of patient medication, prescription information, healthcare insurance status, and other healthcare-related information. It seems that healthcare smart cards have gained increased adoptions and applications in Europe and other countries.

It is envisaged that the HIP facility proposed by this research also contains the appropriate hardware and software functions to cater for smart card

readers and writers to enable smart card use for verification, signing, encryption, and other necessary security applications.

2.7.2 Microsoft Health Vault and Google Health

Recently, Microsoft Health Vault [116] and Google Health [117] have provided health record repositories for individuals to store, manage, access, and share their health information online. Google [117] proclaims that it uses *"electronic security measures such as Secure Socket Layer (SSL) encryption, back-up systems, and other cutting-edge information security technology"* to secure health records. Microsoft [116] also states it uses a variety of security technologies and procedures to protect individual health information, such as HTTPS.[11] Clearly, the safeguards proposed by Google and Microsoft are both non-specific and non-concrete solutions to protect sensitive health information. Both Microsoft and Google allow individuals to read, write, and delete their health records at any time, which leads to concerns over the health record's integrity and accuracy. In addition, such an approach can undermine both healthcare providers' and consumers' confidence and trust in using their online health record systems. Despite this, Australia's National E-health Strategy [3] states that Microsoft and Google play a potentially important role in providing EHR repositories.

2.8 Limitations of existing approaches

This chapter has clearly demonstrated that there has been limited research into overall integrated security architectures for health information systems, as per the proposed OTHIS model. This literature review has identified that specific aspects of the health information system architecture have been the subject of research and discussion for many years; however, existing approaches are unable to identify any major experimental structures developed and tested in this area. This chapter has clearly identified required absent structures for security in each of the major subsystems composing an integrated health information system. This thesis introduces

[11] HTTPS (Hypertext Transfer Protocol Secure) uses Hypertext Transfer Protocol with the SSL/TLS protocol to provide encrypted communications and verification of a network Web Server.

such specific architectural parameters within these broad subsystems, as detailed in Chapters 3 - 8.

2.9 References

[1] H.v.d. Linden, D. Kalra, A. Hasman, J. Talmon, Inter-organizational future proof EHR systems: A review of the security and privacy related issues. International Journal of Medical Informatics, 2009. 78 (3).

[2] National E-health Transition Authority, Privacy Blueprint for the Report on Feedback Individual Electronic, 2008. http://www.nehta.gov.au/component/docman/doc_download/587-privacy-blueprint-for-the-iehr-report-on- (accessed 01/09/2009).

[3] Australian Health Ministers' Advisory Council, National E-Health Strategy Summary, 2008. http://www.health.gov.au/internet/main/publishing.nsf/Content/National+Ehealth+Strategy (accessed 1/09/2009).

[4] H. Mouratidis, P. Giorgini, G. Manson, When security meets software engineering: a case of modelling secure information systems. Information Systems 2005. 30 (8): pp. 609 - 629.

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

[6] P. Ruotsalainen, A cross-platform model for secure Electronic Health Record communication. International Journal of Medical Informatics, 2004. 73 (3): pp. 291-295

[7] D. Gritzalis, C. Lambrinoudakis, A security architecture for interconnecting health information systems. International Journal of Medical Informatics, 2004. 73 (3).

[8] Y.-C. Li, H.-S. Kuo, W.-S. Jian, D.-D. Tang, C.-T. Liu, L. Liu, C.-Y. Hsu, Y.-K. Tan, C.-H. Hu, Building a generic architecture for medical information exchange among healthcare providers. International Journal of Medical Informatics, 2001. 61 (2).

[9] B. Blobel, The European TrustHealth Project experiences with implementing a security infrastructure. International Journal of Medical Informatics, 2000. 60 (2).

[10] E. Smith, J.H.P. Eloff, Security in Health-care Information Systems--Current Trends. 1999. 54 (1): pp. 39-54.

[11] R.J. Anderson, Security in Clinical Information Systems, 1996. http://www.cl.cam.ac.uk/~rja14/policy11/policy11.html (accessed 21/09/2010).

[12] M. Tsiknakis, D. Katehakis, S.C. Orphanoudakis, A health information infrastructure enabling secure access to the life-long multimedia electronic health record, appeared in: Proceedings of the 18th International Congress and Exhibition in Computer Assisted Radiology and Surgery. Chicago, Illinois, USA, (2004)

[13] M. Pfähler, J.H. Weber-Jahnke, Applying an open application security process to a clinical information system: a case study, appeared in: Proceedings of the 2008 C3S2E conference Montreal, Quebec, Canada (2008) Vol. 290.

[14] U.K. National Health Service, Principles of information security, 2010. http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/security (accessed 1/10/2010).

[15] Department of Health and Human Services (HHS), General Overview of Standards for Privacy of Individually Identifiable Health Information, 2003. http://www.hhs.gov/ocr/hipaa/guidelines/overview.pdf (accessed 15/08/2005).

[16] Department of Health and Human Services (HHS), Compliance and Enforcement of the Privacy Rule, 2003. http://www.hhs.gov/ocr/hipaa/conference/compli.pdf (accessed 28/05/2006).

[17] Department of Health and Human Services (HHS), HIPAA Privacy Rule National Conferences 2003. http://www.hhs.gov/ocr/hipaa/conference/intro.pdf (accessed 28/05/2006).

[18] Department of Health and Human Services (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), 2003. http://aspe.hhs.gov/admnismp/FINAL/Fr03-8334.pdf (accessed 10/06/2006).

[19] Department of Health and Human Services (HHS), Information Security Program Health Insurance Portability and Accountability Act (HIPAA) Compliance Guide, 2005. http://csrc.nist.gov/groups/SMA/fasp/documents/pm/HHS_HIPAA_Compliance_Guide_09142005.pdf (accessed 08/10/2010).

[20] R. Leo, ed. The HIPAA Program Reference Handbook. 2005, Auerbach Publications.

[21] National E-health Transition Authority, NEHTA Strategic Plan 2009/10 to 2011/12, 2009. http://www.nehta.gov.au/component/docman/cat_view/219-nehta-stategic-plan (accessed 28/07/2010).

[22] National E-health Transition Authority, Connectivity Architecture Version 1.0, 2008. http://www.nehta.gov.au/component/docman/doc_download/624-connectivity-architecture-v10- (accessed 29/07/2010).

[23] National E-health Transition Authority, Connectivity Architecture Version 1.1, 2010. http://www.nehta.gov.au/component/docman/doc_details/1041-connectivity-introductory-guide-v11 (accessed 29/10/2010).

[24] Canada Health Infoway, EHRS Blueprint Executive Overview, 2006. http://www2.infoway-inforoute.ca/Documents/EHRS-Blueprint-v2-Exec-Overview.pdf (accessed 15/06/2010).

[25] Canada Health Infoway, A "Conceptual" Privacy Impact Assessment (PIA) on Canada's Electronic Health Record Solution (EHRS) Blueprint Version 2, 2008. http://www2.infoway-inforoute.ca/Documents/CHI_625_PIA_rj13.pdf (accessed 19/05/2010).

[26] Canada Health Infoway, An Overview of the Electronic Health Record Privacy and Security Conceptual Architecture, 2006. http://knowledge.infoway-inforoute.ca/EHRSRA/doc/EHR-Privacy-Security-Overview.pdf (accessed 15/06/2010).

[27] National Audit Office, The National Programme for IT in the NHS, 2006. http://www.nao.org.uk (accessed 06/07/2010).

[28] British Broadcasting Corporation (BBC) News, Privacy foes named and shamed, 2004 (accessed 6/11/2010).

[29] R. Spronk, The Spine, an English national programme, 2007. http://www.ringholm.de/docs/00970_en.htm (accessed 30/08/2009).

[30] J. Jürjens, R. Rumm, Model-based security analysis of the German health card architecture. Methods of Information in Medicine, 2008. 47 (5): pp. 409-416.

[31] K.A. Stroetmann, S. Lilischkis, eHealth Strategy and Implementation Activities in Germany, 2007. http://www.ehealth-era.org/database/documents/ERA_Reports/Germany_eH-ERA_Country_Report_final_30-06-2007.pdf (accessed 13/10/2010).

[32] B. Blobel, P. Pharow, A model driven approach for the German health telematics architectural framework and security infrastructure. International Journal of Medical Informatics, 2007. 76 (2): pp. 169 -175.

[33] R. Spronk, AORTA, the Dutch national infrastructure, 2008. http://www.ringholm.de/docs/00980_en.htm (accessed 20/08/2009).

[34] National IT institute for Healthcare, eHealth in the Netherlands - Policies, develoment and status of cross-enterprise information exchange in Dutch healthcare, 2008. http://www.nictiz.nl/uploaded/FILES/Publicaties/Nictiz_eHealth_in_the_Netherlands_June_2008.pdf (accessed

[35] Gartner Inc., Summary of the NHIN Prototype Architecture Contracts, 2007. http://www.hhs.gov/healthit/healthnetwork/resources/summary_report_on_nhin_Prototype_architectures.pdf (accessed 8/09/2010).

[36] The Office of the National Coordinator for Health Information Technology (ONC), Defining Key Health Information Technology Terms, 2008. http://www.hhs.gov/healthit/documents/m20080603/10_2_hit_terms.pdf (accessed 8/09/2010).

[37] M. Scholl, K. Stine, K. Lin, D. Steinberg, Draft Security Architecture Design Process for Health Information Exchanges (HIEs), 2009. http://csrc.nist.gov/publications/drafts/nistir-7497/Draft-NISTIR-7497.pdf (accessed 5/09/2009).

[38] M. Benantar, Access Control Systems Security, Idnetity Management and Trust Models. 2006, Austin TX USA: Springer.

[39] D.F. Ferraiolo, D.R. Kuhn, R. Chandramouli, Role-Based Access Control. 2003, Boston.London: Artech House.

[40] M. Gasser, Building a Secure Computer System. 1988, New York: Van Nostrand Reinhold.

[41] Department of Defense, Trusted Computer System Evaluation Criteria, 1985.

[42] P. Loscocco, S. Smalley, Integrating Flexible Support for Security Policies into the Linux Operating System, appeared in: Proceedings of the FREENIX Track: 2001 USENIX Annual Technical Conference(FREENIX '01)(2001)

[43] P. Loscocco, S. Smalley, Meeting Critical Security Objectives with Security-Enhanced Linux, appeared in: Proceedings of the 2001 Ottawa Linux Symposium(2001)

[44] P. Loscocco, S. Smalley, P.A. Muckelbauer, R.C. Taylor, S.J. Turner, J.F. Farrell, The Inevitability of Failure: the Flawed Assumption of Security in Modern Computing Environments, appeared in: Proceedings of the 21st National Information Systems Security Conference(1998)

[45] D.E. Bell, L.J. LaPadula, Secure Computer Systems: Mathematical Foundations and Model. 1973, The Mitre Corporation.

[46] B. Blobel, Authorisation and access control for electronic health record systems. International Journal of Medical Informatics, 2004. 73 (3): pp. 251-257.

[47] B. Blobel, R. Nordberg, J.M. Davis, P. Pharow, Modelling privilege management and access control. International Journal of Medical Informatics, 2006. 75 (8): pp. 597-623

[48] R. Holbein, S. Teufel, O. Morger, K. Bauknecht, A comprehensive need-to-know access-control system and its application for medical information systems, appeared in: Proceedings of the IFIP TC11 thirteenth international conference on information secuirty. Chapman and Hall, UK, (1997)

[49] J. Reid, I. Cheong, M. Henricksen, J. Smith, A Novel Use of RBAC to Protect Privacy in Distributed Health Care Information Systems, appeared in: Information Security and Privacy, 8th Australasian Conference, ACISP. Wollongong, Australia, (2003)

[50] S. Sucurovic, Implementing security in a distributed web-based EHCR. International Journal of Medical Informatics, 2007. 76 (8): pp. 491-496.

[51] Oracle Corporation, Flexible Mandatory Access Control, 2009. http://hub.opensolaris.org/bin/export/Project+fmac/WebHome?format=pdf (accessed 2/10/2010).

[52] U.S. National Security Agency, Security-Enhanced Linux, 2009. http://www.nsa.gov/research/selinux/index.shtml (accessed 2/10/2010).

[53] M. Henricksen, W. Caelli, P. Croll, Securing Grid Data Using Mandatory Access Controls, appeared in: 5th Australian Symposium on Grid Computing and e-Research (AusGrid). Ballarat Australia, (2007)

[54] L. Xiao, B. Hu, M. Croitoru, P. Lewis, S. Dasmahapatra, A knowledgeable security model for distributed health information systems Computers and Security, 2010. 29 (3): pp. 331-349.

[55] B. Blobel, Comparing approaches for advanced e-health security infrastructures. International Journal of Medical Informatics, 2007. 76 (5-6): pp. 454-459.

[56] E. Weippl, A. Holzinger, A.M. Tjoa, Security aspects of ubiquitous computing in health care. e & i Elektrotechnik und Informationstechnik 2006. 123 (4): pp. 156-161.

[57] A.K. Maji, A. Mukhoty, A.K. Majumdar, J. Mukhopadhyay, S. Sural, S. Paul, B. Majumdar, Security Analysis and Implementation of Web-based Telemedicine Services with a Four-tier Architecture, in: Pervasive Computing Technologies for Healthcare, 2008. PervasiveHealth 2008. Second International Conference (2008).

[58] M.d. Graauw, Implementing Web Services in Dutch Healthcare, 2005. http://www.ringholm.de/docs/03030_en.htm (accessed 7/01/2010).

[59] National E-health Transition Authority, Towards a Secure Messaging Environment, 2006. http://www.nehta.gov.au/index.php?option=com_docman&task=doc_details&gid=63&catid=-2 (accessed 29/09/2010).

[60] National E-health Transition Authority, Example Technical Implementation of Interoperable Web Services - WCFv2.1, 2010. http://www.nehta.gov.au/component/docman/doc_download/1044-example-of-web-services-ws-security-wcf-v21 (accessed 5/10/2010).

[61] National E-health Transition Authority, Example of XML Secured Payload: .NET v1.1, 2010. http://www.nehta.gov.au/component/docman/doc_download/1048-example-of-xml-secured-payload-net-v11 (accessed 5/10/2010).

[62] National E-health Transition Authority, Example of Web Services: TLS: WCF v1.1, 2010. http://www.nehta.gov.au/component/docman/doc_download/1037-example-of-web-services-tls-wcf-v11 (accessed 5/10/2010).

[63] P. Schloeffel, T. Beale, G. Hayworth, S. Heard, H. Leslie, The relationship between CEN 13606, HL7, and openEHR, in: National Health Informatics Conference Sydney, Australia (2006).

[64] National E-health Transition Authority, NEHTA sets direction for electronic messaging in health, . http://www.nehta.gov.au/media-centre/nehta-news/423-nehta-sets-direction-for-electronic-messaging-in-health (accessed 7/10/2010).

[65] B. Blobel, M. Holena, Comparing middleware concepts for advacned healthcare system architectures. International Journal of Medical Informatics, 1997. 46 (2): pp. 69-85.

[66] HL7 Security Working Group, Security Risk Assessmetn Cookbook Version 1.4 Draft, 2009. http://www.hl7.org/Library/Committees/secure/Stds_20090112_SW_7.4_HL7_Security_Cookbook_v1.4_DRAFT.pdf (accessed

[67] B. Blobel, K. Engel, P. Pharow, V. Spiegel, Health Level Seven Security Services Framework Part 2: Fundamentals of HL7 Security (Final Draft), 1999. http://www.hl7.org.au/docs/HL7-Sec.zip (accessed 7/10/2010).

[68] B. Blobel, K. Engel, P. Pharow, V. Spiegel, Health Level Seven Security Services Framework Part 1: Basics of HL7 Security (Final Draft), 1999. http://www.hl7.org.au/docs/HL7-Sec.zip (accessed 7/10/2010).

[69] B. Blobel, V. Spiegel, P. Pharow, K. Engel, R. Krohn, Standard Guide for EDI (HL7) Communication Security Version 1.1, 1999. http://www.hl7.org.au/docs/HL7-Sec.zip (accessed 7/10/2010).

[70] HL7 Security Working Group, ANSI Approved Standards, 2009. http://www.hl7.org/implement/standards/ansiapproved.cfm (accessed 8/10/2010).

[71] ANSI/HL7, HL7 Version 3 Standard: Role-based Access Control Healthcare Permission Catalog, Release 1, 2008. (accessed 30/10/2010).

[72] ANSI/HL7, HL7 Version 3 Standard: Role-based Access Control Healthcare Permission Catalog, Release 2, 2010. (accessed 30/10/2010).

[73] HL7 Security Working Group, HL7 Version 3 Standard: Transport Specification - Web Services Profile, Release 2 2010. http://www.hl7.org/v3ballot/html/infrastructure/transport/transport-wsprofiles.htm#top (accessed 30/10/2010).

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

[75] Privacy Act 1988. 1988: Australia.

[76] Office of the Federal Privacy Commissioner, Federal Privacy Law, http://www.privacy.gov.au/act/index.html (accessed 26/07/2006).

[77] Office of the Federal Privacy Commissioner, Guidelines to the National Privacy Principles, 2001. http://www.privacy.gov.au/publications/nppgl_01.html (accessed 27/07/2006).

[78] National Health and Medical Research Council (NHMRC), Guidelines Under Section 95 of the Privacy Act 1988, 2000. http://www.privacy.gov.au/publications/e26.pdf (accessed 30/07/2006).

[79] National Health and Medical Research Council (NHMRC), Guidelines approved under Section 95A of the Privacy Act 1988, 2001. http://www.privacy.gov.au/materials/types/guidelines/view/7015 (accessed 10/10/2010).

[80] Australian Law reform Commision, ALRC Report 108: For Your Information: Australian Privacy Law and Practice. 2008.

[81] Department of the Prime Minister and Cabinet, Privacy Reforms 2009.

[82] F. Avolio, Firewalls and Internet Security, the Second Hundred (Internet) Years. The Internet Protocol Journal, 1999. 2 (2).

[83] B. Held, Virtual Private Networking - A Construction, Operation and Utilization Guide. 2004, Chichester, England: John Wiley & Sons, Ltd.

[84] R. Pietro, L.V. Mancini, eds. Intrusion Detection Systems. Advances in Information Security, Vol. 38. 2008, Springer.

[85] Australian Health Ministers' Advisory Council, Healthcare Identifiers and Privacy: Discussion paper on Proposals for Legislative Support, 2009. http://www.health.gov.au/internet/main/publishing.nsf/Content/pacd-

ehealth-consultation/$File/Typeset%20discussion%20paper%20-%20public%20release%20version%20070709.pdf (accessed 10/10/2010).

[86] B. Blobel, Onconet: A secure infrastructure to improve cancer patients' care. European Journal of Medical Research, 2000.

[87] B. Blobel, P. Pharow, V. Spiegel, K. Engel, R. Engelbrecht, Securing interoperability between chip card based medical information systems and health networks. International Journal of Medical Informatics, 2001. 64: pp. 401–415.

[88] J. Hu, H.-H. Chen, T.-W. Hou, A hybrid public key infrastructure solution (HPKI) for HIPAA privacy/security regulations. Computer Standards & Interfaces, 2010. 32 (5-6): pp. 274-280.

[89] H. Takeda, Y. Matsumura, S. Kuwat, H. Nakano, J. Shanmai, Z. Qiyan, C. Yufen, H. Kusuoka, M. Matsuoka, An assessment of PKI and networked electronic patient record system: lessons learned from real patient data exchange at the platform of OCHIS (Osaka Community Healthcare Information System). International Journal of Electronic Healthcare 2004. 73 (3): pp. 311—316.

[90] H. Takeda, Y. Matsumura, S. Kuwata, H. Nakano, N. Sakamoto, R. Yamamoto, Architecture for networked electronic patient record systems. International Journal of Medical Informatics, 2000. 60 (2): pp. 161-167.

[91] ISO/IEC 7498-2, Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security architecture.,

[92] J. Carroll, Why standardization is necessary, 2006. http://www.zdnet.com/blog/carroll/why-standardization-is-necessary/1537 (accessed 14/10/2010).

[93] ISO/IEC 7498-1, Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 1: The Basic Model., 1994.

[94] ISO 27799, Health informatics -- Information security management in health using ISO/IEC 27002 2008.

[95] CEN13606, Health informatics - Electronic health record communication - Part 4: Security,

[96] CEN13606, Health informatics - Electronic health record communication - Part 1: Reference model,

[97] CEN13606, Health informatics - Electronic health record communication - Part 2: Archetype interchange specification,

[98] CEN13606, Health informatics - Electronic health record communication - Part 3: Reference archetypes and term lists,

[99] CEN13606, Health informatics - Electronic health record communication - Part 5: Interface specification,

[100] The openEHR Foundation, openEHR Architecture, 2007.

[101] J. Hash, P. Bowen, A. Johnson, C.D. Smith, D.I. Steinberg, NIST SP 800-66, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule,

2008. http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf (accessed 22/10/2010).

[102] National E-health Transition Authority, Connectivity:Implementation Guide Version 1.0 2008. www.nehta.gov.au/.../622-connectivity-implementation-guide-v10- (accessed 5/08/2008).

[103] National E-health Transition Authority, Connectivity Introductory Guide Version 1.1, 2010. http://www.nehta.gov.au/component/docman/doc_download/1041-connectivity-introductory-guide-v11 (accessed 25/10/2010).

[104] National E-health Transition Authority, Connectivity Implementation Guide Version 1.1, 2010. http://www.nehta.gov.au/component/docman/doc_download/622-connectivity-implementation-guide-v10 (accessed 25/10/2010).

[105] Standards Australia, ATS 5820:2010 E-health Web Services Profiles, 2010.

[106] Standards Australia, ATS 5821-2010 E-health XML Secure Payload Profiles, 2010.

[107] Standards Australia, ATS 5822:2010 E-health Secure Message Delivery, 2010.

[108] Standards Australia, TR 5823-2010 Endpoint Location Service, 2010.

[109] National E-health Transition Authority, Service Instance Locator Architecture, 2008. www.nehta.gov.au/.../605-service-instance-locator-architecture-v11-archived (accessed 01/09/2009).

[110] Organization for the Advancement of Structured Information Standards (OASIS), Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of XACML v2.0 for Healthcare Version 1.0, 2009.

[111] Organization for the Advancement of Structured Information Standards (OASIS), Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of Security Assertion Markup Language (SAML) for Healthcare Version 1.0, 2009.

[112] World Wide Web Consortium (W3C), Semantic Annotations for WSDL and XML Schema — Usage Guide, 2007.

[113] World Wide Web Consortium (W3C), Web Services Description Language (WSDL) Version 2.0 SOAP 1.1 Binding 2007.

[114] Frost & Sullivan Market Insight, Smart Cards for Healthcare in Europe, 2010. http://www.frost.com/prod/servlet/market-insight-top.pag?docid=200942088 (accessed 25/10/2010).

[115] R.P. Mampallil, Smart healthcare in Europe. Card Technology Today, 2006. 18 (10): pp. 12-13.

[116] Microsoft Corporation, Microsoft HealthVault Account Privacy Statement, 2010. https://account.healthvault.com/help.aspx?topicid=PrivacyPolicy&culture=en-US (accessed 26/10/2010).

[117] Google, Google Health and HIPAA, 2010. http://static.googleusercontent.com/external_content/untrusted_dlcp/www.google.com/en//intl/en-US/health/Google_Health_and_HIPAA.pdf (accessed 26/10/2010).

Statement of Contribution of Co-Authors for Thesis by Published Paper

In the case of this chapter:

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

Publication status: This paper appeared at Electronic Journal of Health Informatics (eJHI), Vol 3 (1): e3, 2008.

The authors listed below have certified that:

1. They meet the criteria for authorship in that they have participated in the conception, execution, or interpretation, of at least that part of the publication in their field of expertise;
2. They take public responsibility for their part of the publication, except for the responsible author who accepts overall responsibility for the publication;
3. There are no other authors of the publication according to these criteria;
4. There is no conflicts of interest have been disclosed to (a) granting bodies, (b) the editor or publisher of journals or other publications, and (c) the head of the responsible academic unit, and
5. They agree to the use of the publication in the student's thesis and its publication on the Australasian Digital Thesis database consistent with any limitations set by publisher requirements.

Each author's contributions are listed below:

Contributor	Statement of contribution
Vicky Liu	participated in the conception and design of this manuscript, acquisition of data, analysis and interpretation of the data, writing of this manuscript and acting as the corresponding author
Lauren May	supervised to the conception and design of this manuscript and revising it critically for important intellectual content
William Caelli	contributed to the conception and design of this manuscript, revising it critically for important intellectual content and final approval of the version to be published
Peter Croll	performed data acquisition on literature review information

Principal Supervisor Confirmation

I have sighted email or other correspondence from all co-authors confirming their certifying authorship.

W CAELLI
Name


Signature

12-8-2010
Date

Chapter 3 Strengthening Legal Compliance for Privacy in Electronic Health Information Systems: A Review and Analysis

Vicky Liu, Lauren May, William Caelli, and Peter Croll
Information Security Institute, Faculty of Information Technology
Queensland University of Technology, Australia

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 also 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

The *electronic Journal of Health Informatics* is an international journal committed to scholarly excellence and dedicated to the advancement of Health Informatics and information technology in healthcare. ISSN: 1446-4381

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

3.1 Introduction

Modern societies are inextricably dependent upon information. Information is data managed by information systems in some sort of useful way. The effective management of information, therefore, is a major key factor in attaining maximum value from our information systems. As with the majority of society's information systems, health information systems evolved historically, before computers became widely available, as manual- and paper-based systems. As health information is sensitive by nature these traditional manual systems have, in general, coped with privacy, security, integrity and confidentiality issues through the professionalism of their management staff, trustworthy people applying developed procedures.

In the broad sense today's electronic information systems are comprised of people, processes and technologies that come together in some meaningful way. This paper does not attempt to cover all aspects of such systems. The people aspects such as staffing guidelines, qualifications, etc are well outside the scope of this paper, as are procedures and processes of these systems such as limitations of the collection, use and disclosure of health data, anonymity and consent. This paper is primarily concerned with the technological aspects of such systems, the ICT technologies which provide the foundational basis of health electronic information systems. The specific focus is on viable ICT systems which can improve upon current techniques of access control in health systems. The term "access control" in this paper refers to the concept in the broader sense, rather than perhaps the more common narrow view of access control meaning an application password.

Information systems are created specifically to assist in the practicalities of managing this information. The move to the electronic system, however, does not inherently retain the human qualities implicit in the manual system. For example, how does one replicate the intrinsically human qualities of "professionalism" and "trust" in a computing system? In the strict technical sense, trust and trustworthiness of electronic systems are very complex areas of research, which are well outside the scope of this paper. These terms are used in this paper as the generic commonly-accepted perception of human-computer-human trust which reflects the open literature in this context.

In the progression from manual to electronic systems, major issues can arise with respect to privacy and security, particularly for applications where privacy and security are high priority requirements. Health information systems are a prime example. Historically information protection and trust is inherent in paper-based systems through the personal integrity of the system's management staff. Society trusts its health professionals to do the right thing. In general the manual system is a very trustworthy system. The central theme of this paper is concerned with how the trust which is inherent in the manual system transfers to trust in the digital world. As the authors demonstrate in later sections this is not as simple a process as it sounds. Trust in the human sense is an analog measure. People generally trust by degrees and can make good decisions efficiently, based upon some fairly complex scenarios, especially where the person is very experienced in the area. Digital trust however is quite simplistic in that it is binary by nature, either yes or no, with no real sense of `experience' or `history'. The research question is: How well can we incorporate human-type trust in our health information systems?

Section 3.3.2 identifies current electronic health information system concerns and considerations in modern society. This is primarily an issue for the health sector because electronic health information systems are developed using commodity general-purpose computers which do not, in general, give high priority to privacy and security requirements. The authors advocate that the majority of these issues can be effectively addressed through improving

the basis of trust in the health digital world. Why hasn't this already been done? To date trusted computing systems have remained solely in the realms of experimental research or have been proprietarily developed in-house for specific high-security applications. The authors believe that aspects of this research have developed to such an extent that trusted computing foundations for the more general health sector are now a feasible option. This paper is primarily concerned with proposing a trusted computing foundation for the health sector. The proposals discussed are offered as viable options towards which current health systems could evolve from their current position. This research is designed to emphasise to health information system professionals that common goals of enhanced security and privacy of information are achievable with today's technology, and without the need for drastic changes to health information systems. An adjustment in focus of relevant developers can gently evolve current foundational systems into more trusted bases for health information systems by directing development efforts towards the concepts discussed in this paper.

What do we mean by a computing foundation? The hardware components of computer systems including the disk drive, the keyboard, the monitor and the printer, are managed at the foundational level by an operating system which is typically comprised of basic software and firmware. The operating system, then, is responsible for the basic way in which a computer works and operates. Different operating systems run on the same hardware will effectively produce different computing systems. Trusted operating systems give high priority to privacy and security features.

All information systems are developed atop the operating systems of the computer. These applications can make use of the operating system features. Currently health information systems make use of generic operating systems. Since privacy and security issues do not rate highly in the priorities of generic operating systems these applications are inherently susceptible to privacy and security compromise. The majority of health information system issues that we see today can be overcome by adopting more security-aware operating systems.

The authors propose that health information systems should be developed and operated upon trusted operating systems so that these applications can exploit the inherent privacy and security features in the underlying operating systems. Trusted health information systems are definitely the way forward. The health sector is at a turning point in its evolution. Feeding into that juncture is the current status of e-health systems globally, the need to satisfy privacy legislation, standardisation and implementation constraints, and the desire to implement national unified electronic healthcare systems. Moving forward from this juncture is the trusted health information system, which is developed atop the trusted operating system.

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.

Section 3.3.2 introduces the purpose of this research and positions the role of trusted operating systems in the global health information systems sector.

Section 3.3.3 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 3.3.4 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 effect on every information system that uses or processes health information in the USA.

Section 3.3.5 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 3.3.6 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 3.3.7.

3.2 Security and Privacy

3.2.1 Information Security

While “security” and “privacy” are very closely related, they are two distinct concepts. Throughout this paper these terms are used primarily in their technical sense. Consequently we define what we mean by security and privacy in this section.

Beaver and Herold [1] argue that “Security is tactical strategy. Privacy is a contextual strategic objective” and “Security is the strategy. Privacy is the outcome”. Implementing security policies ensures privacy and using security strategies obtains privacy. The traditional goals of information security are confidentiality and integrity in addition to non-repudiation. The word "security" is a generic term covering many aspects which one may or may not desire in an application. The idea of a "security application" is to incorporate the required security aspects into its design and development.

Privacy is a "people" concept. It is “the right of individuals to be left alone and to be protected against physical or psychological invasion or the misuse of their property” [2]. It is also “… an individual’s desire to limit the disclosure of personal information” [3]. For electronic health records, effective privacy provides the freedom and ability to share an individual’s personal and health information in confidence. Privacy in health is an area of high sensitivity and can present one of the major obstacles preventing electronic health records from being trusted and hence adopted.

3.2.2 E-Health and Privacy

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 [4] 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.

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 active in e-health. 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.

3.3 Current and previous e-Health Management Systems

3.3.1 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 at

a national level. This gives a true perspective to real-world current issues which need addressing. One may argue that since Australia's health system is different to another country's health system there is little to be gained from inspecting health systems internationally. Our justification is that, regardless of the actual health system application (be it UK, USA or Australia), common inherent requirements in any health information system are the ability to provide security and privacy features as and where required. By building such applications atop a common trusted operating system, each individual application can use the inherent security and privacy features of the operating system whilst simultaneously developing proprietary software for its own specific national requirements. This paper is primarily concerned with proposing a trusted computing foundation for the health sector.

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[13]. Its goal is to connect 8,000 surgeries, 240 hospitals, 100,000 doctors and 380,000 nurses 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 states and territories have their own individual programs. The current national e-health strategy is "HealthConnect"[14] 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[15][16][17].

[13] 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.
[14] "What is happening – National" is available at http://www.health.gov.au/internet/hconnect/publishing.nsf/Content/national-1lp, accessed 09/07/2006.
[15] More D., "HealthConnect - A Major Rethink Required?" is available at http://www.newmatilda.com/policytoolkit/policydetail.asp?PolicyID=106, accessed 16/07/2006.

3.3.2 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 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 [5] 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 [6] states that successful implementation of electronic record systems must learn from the UK's previous health strategy experience. Quinne[18] 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

[16] Howarth, B., "Australia's e-records mess" is available at http://www.govhealthit.com/article94797-06-12-06-Print accessed 15/07/2006.
[17] 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.
[18] 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

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.

3.4 An Overview of Privacy Laws and Legislation 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 3.3.1 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 3.3.2 outlines the Australian Federal Privacy Act and relevant Australian State/Territory privacy laws and health record legislation.

3.4.1 USA Privacy Laws and Health-related Privacy Legislation

3.4.1.1 HIPAA Overview

HIPAA [7] 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)"* [8].

3.4.1.2 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 [9]. 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 [8].

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 [8] .

3.4.1.3 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 although there are strict rules and tests for the de-identification process. 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 Rule [8].

The Privacy Rule defines situations or purposes for which the permitted uses and disclosures of PHI. There are also civil, monetary and criminal penalties for failure to comply with the Privacy Rule apply. 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 [9] .

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 [8].

3.4.1.4 Security Rule and Privacy Rule – “No security, no privacy”

Beaver and Herold [1] 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 [8].

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 [8].

3.4.1.5 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 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.

There are numerous security enhancing techniques available, such as digital signature or checksum technologies, that ensure 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[19] systems

[19] 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

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[20]), Network Layer Security (IPSec[21]) and Secure Sockets Layer (SSL[22])/Transport Layer Security (TLS[23]) 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 [10].

3.4.2 Australian Privacy Laws and Health-related Privacy Legislation

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

3.4.2.1 Australian Federal Government

The principal Federal statute is the Privacy Act 1988 [11] which has provisions for the protection of the privacy of personal information including eleven *"Information Privacy Principles (IPPs)".* The Commonwealth and Australian Capital Territory (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

---

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.

[20] 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.

[21] 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.microsft.com/windowsserver2003/technologies/networking/ipsec/default.mspx accessed 22/11/2005.

[22] 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.

[23] 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.

information including the ability to grant individuals certain rights to access their personal information and correct errors [12].

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 [13].

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 [14] and s.95A [15] 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 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 s.95 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 s.95A applies to medical research that involves access to personal information held by organisations in the private sector.

3.4.2.2 Commonwealth/Federal – State and Territory Privacy Acts

Table 4Table 4: General structure of privacy legislation in Australia indicates the general structure of the privacy legislation in Australia.

Jurisdiction	Law-Regulation-Code-Standard	Covered Entity	Effective Date	Relevant Guidelines
Cth	Privacy Act 1988 http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/pages/PNSW_03_ppipact	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 law nor administrative privacy regime** Information Privacy Bill 2007	With the Bill, the Information Privacy Principles are applied to the public sector; the Health Privacy Principles are applied to both public and private sectors	Mar-2007	
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 http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/pages/PNSW_03_ppipact	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	

Table 4: General structure of privacy legislation in Australia

3.4.2.3 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[24] (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

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

legislation in Australia includes the Commonwealth Privacy Act. As indicated in Table 4, 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. In 28 March 2007, Western Australia introduced the Information Privacy Bill 2007 into parliament. There are no specifically independent laws to address the privacy of health information in QLD and SA, but these states have administrative standards and obligations. Fernando [16] 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 [17]. 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.

3.5 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.

3.5.1 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) [18] (often cited as the "Orange Book" with associated documents known as the "Rainbow Series"), the European Information Technology Security Evaluation Criteria (ITSEC) [19], and the Canadian Trusted Computer Product Evaluation Criteria[25] (CTCPEC).

These evaluation criteria, along with others, have been largely superseded by the internationally accepted *"Common Criteria (CC)"* for such evaluation [20]. 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, 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.

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

3.5.2 Essential Concepts of the CC

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 [21].

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

3.5.2.1 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 [21].

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 [22].

3.5.3 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 card related devices and systems and other application needs. In relation to the privacy of healthcare an examination of relevant operating system and access control related PPs is needed. This includes:

- Controlled Access PP (CAPP),
- Labelled Security PP (LSPP),
- Role Based Access Control PP (RBAC PP), and
- Healthcare systems related PPs.

3.5.3.1 Controlled Access Protection Profile (CAPP)

Firstly, the assurance level of the CAPP [23] 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.

3.5.3.2 Labelled Security Protection Profile (LSPP)

The assurance level of the LSPP [24] is “EAL 3 augmented”. LSPP conformant products should support two classes of access control mechanism, DAC, and *“Mandatory Access Control (MAC)”*. With the MAC policy, the overriding information access rule is based on the concept of “clearances” for users and “classifications” 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.

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

The assurance level of the RBAC PP [25] 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.

3.5.3.4 Health Related Protection Profiles

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[26] has been under development

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

since 1999 but, unfortunately, no published protection profile for healthcare has eventuated. To date, the only two health related protection profiles that have been published are the Protection Profile for electronic Health Card (PP eHC) [26] and the Protection Profile for Health Professional Card (PP HPC) [27]. 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.

3.5.4 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 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 limitations 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.

3.6 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 usually 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 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[27]*"* for the implementation of national

[27] "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.

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[28] (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. A literature analysis has failed to indicate any major trend in this area.

3.7 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 as a major impediment to current and previous systems. The healthcare management system is then developed atop the secure MAC-based operating system.

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

This paper has reviewed current ICT security architectures and standards. Military, government and financial institutions demand the highest level of security standard for their strict security requirements. The health sector, handling sensitive personal information and providing critical health services, should also insist on the highest level of security. 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 "commercial off-the-shelf (COTS)[29]" [28]. It is also recommended that any application or subsystem responsible for the security enforcement activities for individually identifiable health information must be evaluated at a level of "EAL5" at least, and preferably higher. This would include, in particular, any appropriate cryptographic subsystems for such usage. Commercial computer and network systems currently, or soon will, exist to meet these requirements. Exemplary mainstream operating systems include:

- "Red Hat Enterprise Linux (RHEL) Version 5", and
- "Sun Microsystems Solaris 10 with Trusted Extensions Software" and others.

In June 2007, RHEL Version 5 running on IBM systems achieved CC "EAL 4+" augmented with ALC_FLR.3 (assurance life-cycle flaw remediation) certification with conformance to the LSPP CAPP and RBAC PP[30]. To date the Sun Microsystems Solaris 10 Operating System (OS) has entered into

[29] Commercial off-the-shield (COTS) refers to commercial products such as computer hardware, software, components or subsystems which are manufactured commercially for sale. COTS products are different from in-house developments tailored to suit specific requirements. A definition of COTS can be found at http://en.wikipedia.org/wiki/Commercial_off-the-shelf accessed 10/07/2007.

[30] RHEL Version 5 operating on IBM systems is recently certified at EAL 4 Augmented for LSPP, CAPP, and RBAC PP with ALC_FLR.3 certification available at http://niap.bahialab.com/cc-scheme/vpl/ accessed 10/07/2007.

evaluation for CC certification at “EAL 4+”. Currently, Sun’s Trusted Solaris 8 OS is certified at “EAL 4+” for LSPP, CAPP and RBAC PP.

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 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 3 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, firmware and hardware.

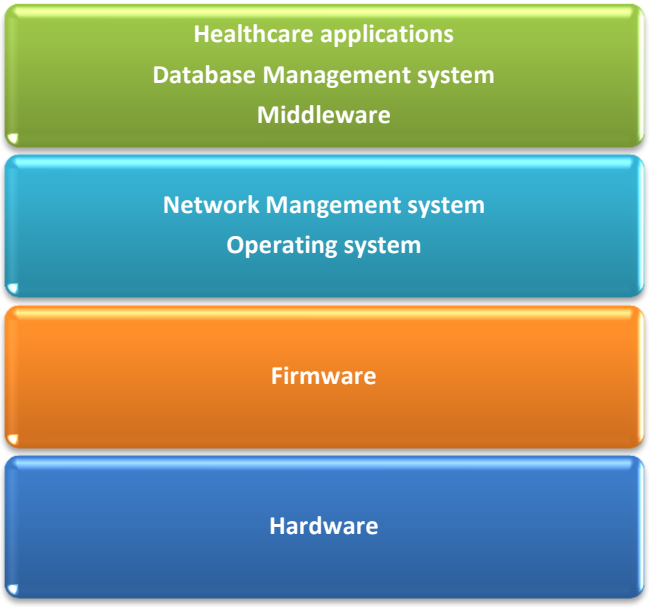


Figure 3: Health information system architecture

Security may be implemented at the level of the health services applications system. Even if security is established within that health services 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 depends 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 are considered 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 [29] 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 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 five years.

3.8 References

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

[2] Institute of Medicine, The Computer-Based Patient Record: An Essential Technology for Health Care, Revised Edition. 1997: National Academy Press.

[3] National Research Council, For the Record: Protecting Electronic Health Information. 1997: National Academy Press.

[4] NHS, The Use Of Computers In Health Care Can Reduce Errors, Improve Patient Safety, And Enhance The Quality Of Service - There Is Evidence, 2005. http://www.connectingforhealth.nhs.uk/worldview/protti2/ (accessed 17/08/2006).

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

[6] M. Carter, Integrated Electronic Health Records and Patient Privacy: Possible Benefits but Real Dangers, 2000. http://www.mja.com.au/public/issues/172_01_030100/carter/carter.html#subr0 (accessed 17/07/2005).

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

[8] Department of Health and Human Services (HHS), Information Security Program Health Insurance Portability and Accountability Act (HIPAA) Compliance Guide, 2005. http://csrc.nist.gov/groups/SMA/fasp/documents/pm/HHS_HIPAA_Compliance_Guide_09142005.pdf (accessed 08/10/2010).

[9] Department of Health and Human Services (HHS), HIPAA Administrative Simplification Compliance Deadlines, 2003. http://www.cms.hhs.gov/HIPAAGenInfo/Downloads/HIPAAComplianceDeadlines.pdf (accessed 12/06/2006).

[10] Department of Health and Human Services (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), 2003. http://aspe.hhs.gov/admnismp/FINAL/Fr03-8334.pdf (accessed 10/06/2006).

[11] Privacy Act 1988. 1988: Australia.

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

[13] OFPC, Guidelines to the National Privacy Principles, 2001. http://www.privacy.gov.au/publications/nppgl_01.html (accessed 27/07/2006).

[14] National Health and Medical Research Council (NHMRC), Guidelines Under Section 95 of the Privacy Act 1988, 2000. http://www.privacy.gov.au/publications/e26.pdf (accessed 30/07/2006).

[15] National Health and Medical Research Council (NHMRC), Guidelines approved under Section 95A of the Privacy Act 1988, 2001. http://www.privacy.gov.au/materials/types/guidelines/view/7015 (accessed 10/10/2010).

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

[17] DoHA, The Proposed National Health Privacy Code, 2003. http://www7.health.gov.au/pubs/nhpcode.htm (accessed 11/07/2005).

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

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

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

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

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

[23] NSA, Controlled Access Protection Profile Version 1.d, 1999. http://niap.nist.gov/cc-scheme/pp/PP_CAPP_V1.d.pdf (accessed 18/10/2005).

[24] NSA, Lablled Security Protestion Profile Version 1b, 1999. http://niap.nist.gov/cc-scheme/pp/PP_LSPP_V1.b.pdf (accessed 18/10/2005).

[25] J. Reynolds, R. Chandramouli, Role-Based Access Control Protection Profile Version 1.0, 1998. http://www.cesg.gov.uk/site/iacs/itsec/media/protection-profiles/RBAC_987.pdf (accessed 18/10/2005).

[26] BSI, Common Criteria Protection Profile electronic Health Card (eHC) – elektronische Gesundheitskarte (eGK), 2005. http://www.bsi.de/zertifiz/zert/reporte/PP0020b.pdf (accessed 08/08/2006).

[27] BSI, Common Criteria Protection Profile Health Professional Card (HPC) Heilberufsausweis (HPA), 2005. http://www.bsi.de/zertifiz/zert/reporte/PP0018b.pdf (accessed 08/08/2006).

[28] TNOITSEF, Developers | list of evaluated products, http://www.commoncriteriaportal.org/public/developer/index.php (accessed 08/08/2006).

[29] P. Loscocco, S. Smalley, P.A. Muckelbauer, R.C. Taylor, S.J. Turner, J.F. Farrell, The Inevitability of Failure: the Flawed Assumption of Security in Modern Computing Environments, appeared in: Proceedings of the 21st National Information Systems Security Conference(1998)

Statement of Contribution of Co-Authors for Thesis by Published Paper

In the case of this chapter:

Publication title: A Sustainable Approach to Security and Privacy in Health Information Systems

Publication status: This paper appeared at 18th Australasian Conference on Information Systems (ACIS 2007), Toowoomba Australia.

The authors listed below have certified that:

1. They meet the criteria for authorship in that they have participated in the conception, execution, or interpretation, of at least that part of the publication in their field of expertise;
2. They take public responsibility for their part of the publication, except for the responsible author who accepts overall responsibility for the publication;
3. There are no other authors of the publication according to these criteria;
4. There is no conflicts of interest have been disclosed to (a) granting bodies, (b) the editor or publisher of journals or other publications, and (c) the head of the responsible academic unit, and
5. They agree to the use of the publication in the student's thesis and its publication on the Australasian Digital Thesis database consistent with any limitations set by publisher requirements.

Each author's contributions are listed below:

Contributor	Statement of contribution
Vicky Liu	participated in the conception and design of this manuscript, acquisition of data, analysis and interpretation of the data, writing of this manuscript and acting as the corresponding author
Lauren May	supervised to the conception and design of this manuscript and revising it critically for important intellectual content
William Caelli	contributed to the conception and design of this manuscript, revising it critically for important intellectual content and final approval of the version to be published
Peter Croll	performed data acquisition on literature review information

Principal Supervisor Confirmation

I have sighted email or other correspondence from all co-authors confirming their certifying authorship.

W. CAELLI
Name

Signature

12-8-2010
Date

Chapter 4 A Sustainable Approach to Security and Privacy in Health Information Systems

Vicky Liu, Lauren May, William Caelli and Peter Croll
Faculty of Information Technology and Information Security Institute
Queensland University of Technology, Australia
Email: {v.liu, l.may, w.caelli, croll}@qut.edu.au

Abstract

This paper identifies and discusses recent information privacy violations or weaknesses which have been found in national infrastructure systems in Australia, the United Kingdom (UK) and the United States of America (USA), two of which involve departments of health and social services. The feasibility of health information systems (HIS) based upon intrinsically more secure technological architectures than those in general use in today's marketplace is investigated. We propose a viable and sustainable IT solution which addresses the privacy and security concerns at all levels in HIS with a focus on trustworthy access control mechanisms.

Keywords: access control, trusted systems, information assurance, health information systems

4.1 Introduction

Today's service industries would regard information, computer and telecommunication (ICT) technologies as part of their critical infrastructure. Although some sectors such as healthcare, have been slow in their adoption of ICT, it is evident they are working towards a future where ICT technologies will be both widespread and essential. 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. Notwithstanding the obvious potential advantages of deploying ICT in

18th Australasian Conference on Information Systems
5-7 Dec 2007, Toowoomba

healthcare services, there are some concerns associated with integration of and access to electronic health records. Information stored within electronic health systems is highly sensitive by its very nature, therefore health records have clear requirements for confidentiality in order to safeguard personal privacy and to maintain record integrity.

A security violation in a health information system (HIS), such as an unauthorised disclosure or unauthorised alteration of individual health information, has the potential for disaster among healthcare providers and consumers. Although the concept of Electronic Health Records (EHR) has much potential for improving the processing of health data, Goldschmidt [1] warns that electronic health records may also pose new threats for compromising sensitive personal health data if not designed and managed effectively. Goldschmidt also illustrates that malevolent motivations could feasibly disclose confidential personal health information on a more massive scale and at a higher speed than possible with traditional paper-based medical records. Quinn suggests that the key factor to successful implementation of a national health information system is user adoption [2]. User acceptability and adoption 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 accept and adopt a new technology that does not always facilitate efficient working practices. To encourage healthcare service consumers and providers to use electronic health records, it is crucial to instil confidence that the electronic health information is well protected and that consumers' privacy is assured.

Several countries including Australia, the UK, the USA, Canada and New Zealand are actively involved in the development of e-health initiatives. The current approaches to protecting personal privacy and confidentiality of electronic patient records are, in the opinion of the authors, not sustainable. This paper identifies and discusses three scenarios related to information privacy violations or weaknesses which have recently been found in Australia, the UK and the USA. The paper proposes a viable ICT solution to provide appropriate levels of secure access control for the protection of sensitive

health data. Increasingly, HIS are being developed and deployed based upon commercial, commodity-level ICT products and systems. Such general-purpose systems have been created over the last 25 years with often only the minimal security functionality and verification. In particular access control, a vital security function in any operating system that forms the basis for application packages, has been founded upon earlier designs based on an access control method known as Discretionary Access Control (DAC) as described in later sections. DAC systems were defined around an environment where data and program resources were developed and deployed within a single enterprise, assuming implicit trust amongst users. This environmental model is no longer valid for modern HIS. In some commercial systems, for example, even the addition of a simple single printer unit has the capacity to seriously undermine the overall integrity of the information system.

This paper investigates the feasibility of HIS based upon intrinsically more secure technological architectures than those in general use in today's marketplace. Even though such systems are currently commercially available for enterprise system deployment, for example SELinux, they are not in widespread use. The privacy and security issues required of HIS applications are analysed in the context of a new approach to a more trustworthy structure, the Open Trusted Health Informatics Scheme (OTHIS). This scheme consists of a number of trusted models including the Health Informatics Access Control (HIAC) system which is discussed in detail.

4.2 Access Control

Access control is one of the fundamental security mechanisms used to protect computer resources, in particular in multi-user and resource-sharing computer environments. “Access control” simply refers to a set of rules that specify which users can access what resources with which types of access restrictions. Various operating systems, network control systems, and database management systems (DBMS) can employ a choice of access control mechanisms to allow admission of a user to access protected resources of the system. It should be noted that in any information system a

distinction may be made between “security aware applications” and “security ignorant applications”. These latter applications usually depend solely upon access control facilities provided by an operating system, DBMS and other like middleware. Controlling appropriate access to data in any information system is a major security issue. Many instances of poor access control management practices leading to security and privacy violations are reported on a regular basis. Recent occurrences include:

4.2.1 Scenario 1: Privacy Invasion Scandal at Australia’s Centrelink

Australia’s Centrelink, a Commonwealth Government agency, delivers a range of social welfare services and payments to the Australian community including issuing Health Care Cards for concessions on healthcare costs. In carrying out its duties, Centrelink officers may verify information on personal financial and tax records with the Australian Taxation Office (ATO). According to a published media article [3], Centrelink conducted a two-year investigation on invasion of privacy by deploying spyware technology to audit and monitor employees’ access to client records. The results of this investigation found 790 cases of inappropriate access to client records since 2004. Consequently, 19 IT staff were dismissed, 92 resigned, more than 300 staff faced salary deductions or fines, another 46 were reprimanded and the remainder were demoted or warned. Introduction of the proposed Medical access card in Australia, which may encompass healthcare parameters as well as social security information, is particularly concerning given the findings of this investigation.

Analysis 1: The information collected and stored by Centrelink is of a highly sensitive nature. It is therefore essential that the privacy and integrity of such information is safeguarded from internal and external security threats and attacks. Centrelink deploys spyware software to detect inappropriate access to client records and enforces the penalty for persons convicted in breach, however such steps only deal with occurrences of privacy violations in a reactive manner. It is preferable to adopt a proactive tamper resistant protection approach where such incidents simply cannot occur. The authors

propose that this can be achieved by employing the appropriate technological controls to prevent unauthorised access or alteration of the private information ensuring individuals' privacy and integrity of their information.

4.2.2 Scenario 2: A Lack of Adequate Safeguards to Access UK NHS Patient Records

The current UK National Programme for IT (NPfIT) is considered to be the world's largest ICT project providing an HIS for 50 million patients. It has been reported by the media [4] that a lack of adequate security measures is in place regarding providing access to shared patient records once they are on the national database system. Patient records may contain sensitive information such as mental illness, abortions, pregnancy, HIV status, drug-taking or alcoholism. The article warns that the 50 million patient records may be made accessible by up to 250,000 National Health Services (NHS) staff including police and health managers, counsellors, social workers, private medical practices, ambulance staff and commercial researchers. This has resulted in calls for a boycott of patient records accessible by thousands of authorised NHS staff.

Analysis 2: The confidentiality management approach deployed by the UK NHS to access patient records will be on a "need-to-know" basis. Varied access permissions, based on the role-based access policy, will be granted to access patient records. In its basic form this is a simplistic approach which will not satisfactorily address the primary issue of a lack of adequate safeguards. In particular this approach does not allow patients to selectively protect particular parts of their uploaded information from being widely accessed. NHS declares that a "sealed envelope" [5] mechanism will allow patients to express access restrictions on disclosure of their confidential health information from specific roles. The provision of sealed envelopes however will not be available until the second phase of the release of the NHS Care Record Service.

4.2.3 Scenario 3: Significant IT Security Weaknesses Identified at USA HHS Information Systems

A published security analysis report from the United States Government Accountability Office (GAO) [6] assessed the effectiveness of the Department of Health and Human Services (HHS) information security program with emphasis on the Centers for Medicare and Medicaid Services (CMS). The GAO's report reveals numerous significant security weaknesses in the areas of network management, user accounts and passwords, user rights and file permissions, and the auditing and monitoring of security-related events, specifically with HHS unnecessarily granting access rights and permissions to sensitive files and directories.

HHS provides essential health and welfare services to the USA community. CMS, a major operating division within HHS, is responsible for the Medicare and Medicaid programs. HHS is highly reliant on networked information systems to carry out their services including processing medical claims, conducting medical research, managing health and disease prevention, and a food safety program. Because such information systems contain sensitive medical and financial information, it is essential that the security and integrity of such information systems are safeguarded from security threats and vulnerabilities.

Analysis 3: The identified security weaknesses in the HHS information systems increase the very high risk that unauthorised users can gain access to and subvert the systems upon which HHS relies to deliver its vital services. Not surprisingly, this has the potential to expose clients' sensitive information to serious privacy invasions. GAO's recommendation [6] to HHS is to implement a complete set of comprehensive information security programs at all operating divisions to address the identified weaknesses.

The three illustrated scenarios all have a common security weakness issue which is directly related to access control management. Appropriate computer-based access control schemes can be deployed to address these information security issues. Access control mechanisms, then, are used to

restrict users' accesses to resources. Organisations use these controls to grant employees the authority to access only the information the users need to perform their duties. Access controls can limit the activities that an employee can perform on data. Before proposing a viable solution to provide appropriate levels of secure access control for protecting sensitive health data, one must first understand the primary types of computer-based access control. These are examined in the following section.

4.3 Access Control models

The two traditional types of access control modes are Discretionary Access Control (DAC) and Mandatory Access Control (MAC). The Role-Based Access Control (RBAC) concept is complementary to both DAC and MAC techniques. RBAC enables easier management by ensuring finer granularity in the access system.

4.3.1 Discretionary Access Control (DAC)

The DAC mechanism is widely implemented for the purpose of managing access control by current commodity software such as Microsoft Corporation's Windows systems, open-source systems such as Linux and the original Unix system. The DAC policy allows the owner of information to grant access permissions to other users or programs at his/her discretion without the system administrator's knowledge. Each user has complete discretion over his/her own objects. Thus, such a policy does not provide the actual owner of the system fully centralised access control over the organisational resources. In fact, the system cannot identify the difference between a legitimate request to modify access control information which originated from the owner of the information and a request issued by a malicious program [7].

DAC mechanisms are fundamentally inadequate for strong system security. One of the major deficiencies with DAC is its vulnerability to some types of Trojan horse attacks. Trojan horses embedded in applications can exploit DAC's vulnerability to cause an illegal flow of information. Applications that rely on DAC mechanisms are vulnerable to tampering and bypassing [8].

Malicious or flawed applications can easily cause security violations in the system. This shortcoming of DAC can be overcome by employing MAC policies to prevent information flow from higher to lower security levels.

4.3.2 Mandatory Access Control (MAC)

Gasser [7] states that MAC can be used to prevent some types of Trojan horse attacks by imposing severe access restrictions that cannot be bypassed intentionally or accidentally. MAC can provide the ability to limit access to only legitimate users. Ferraiolo et al [9] underscore that MAC is necessary when provision of a truly secure system is required.

With MAC, each user possesses a clearance that is used by the system to determine whether a user can access a particular file. Access permissions are determined by a user's clearance compared with the sensitivity (or security) or classification level label on information stored in the system, not upon the user's discretion. The classification may contain an arbitrary number of categories; for example a conventional hierarchical category set used in military environments might include "top secret", "secret", "confidential" and "unclassified". Each user possesses a clearance that is used by the system to determine whether a user can access a particular file. The access permission to information is determined by the user's clearance compared to the security level of information stored in the system. This is also known as a multi-level security (MLS) policy, which was first introduced by Bell and LaPadula (BLP) [10].

With the MLS policy, BLP propose an access control system in the form of a mathematical model for defining and evaluating computer security. This model is designed to address the enforcement of information confidentiality aimed at the prevention of unauthorised information leakage. The BLP model defines two basic rules for making access control decisions: the Simple property and the Star property. The Simple property regulates whether a subject is allowed to read an object (i.e. if the subject's clearance level dominates the security level of the object). It is also known as the "no read up" policy. The Star property determines whether a subject is allowed

to write to an object (i.e. if the security level of the object dominates the subject's security clearance level). It is referred to as the "no write down" policy [7, 9].

The traditional MAC policy was originally designed for a military environment based on the MLS hierarchical structure and was quite rigid in its application. More recent research has modernised the traditional MAC approach, overcoming its traditional limitations, in order to better suit contemporary applications such as for the HIS environment.

4.3.3 Role-based Access Control (RBAC)

RBAC is based upon the role concept in managing access control where access permissions are associated with roles. Users are assigned to appropriate roles within the organisation. The user must be assigned as a member of a role in order to perform an operation on an object. Ferraiolo et al [9] state that the driving force behind the RBAC model is to simplify the management of authorisation. Assigning users' access permissions to each protected object in the system on an individual user basis, particularly in large scale enterprise systems, is an onerous process in security management. With RBAC, users are granted membership into roles according to their responsibilities and competencies. User membership of roles can be included and revoked easily. Updates of assigning privileges can be done to roles rather than updating permission assignments for individual users. RBAC supports users' access rights based on such parameters as job function, enforcement of least privilege for administrators and users, enforcement of static/dynamic separation of duties (SOD) and hierarchical definitions of roles.

In spite of several advanced RBAC features, RBAC also brings a number of limitations. Significantly, Reid et al [11] point out that RBAC does not efficiently support access policies in the way of general consent qualified by explicit denials. This issue is quite apparent in the privacy vulnerability that occurred in the UK NHS patient record system analysed in Scenario 2. There is also a lack of available products to support the full features of RBAC.

A number of research papers discuss the use of the RBAC mechanism for authorisation management in healthcare environments, since role models are suitable for the representation of roles in hospital settings. Ferraiolo et al [9], the developers of the first model for RBAC and proposers of the RBAC standard, state that RBAC is policy-independent and policy neutral in not enforcing any particular protection policy. Ferraiolo et al also point out that the availability of RBAC does not obviate the need for MAC and DAC policies. MAC is particularly needed when confidentiality and information flow are primary concerns.

4.3.4 Rethink Access Control Models in HIS

Current moves toward Web-based identity and authentication structures present a major challenge where such structures are not based on highly trusted operating systems. All applications and supporting software which necessarily reside atop the untrusted operating systems are also untrusted. We emphasise the need for further research into, and redefinition of, MAC in light of modern information system structures, legislative and regulatory requirements and flexible operational demands in HIS.

Building upon experience with DAC and MAC structures, indications are that a radical re-think is required in the understanding of access control in general in current and future information systems, and in particular in the healthcare environment. One limiting factor in approaches to “hardening” current information systems is the perceived or expected business requirements to maintain backward compatibility for legacy applications [12].

Any access control system fundamentally depends upon a trusted base for safe and reliable operation, commonly referred to as a “trusted computing-base (TCB)”. Without a TCB, any control structures are subject to compromise. In the past, access control paradigms have been based around fundamentals in operating systems, DBMS and similar IT products. With the ubiquity of information systems, this paper proposes that access control requirements need to be defined against the background of the relevant industries served by such systems.

4.4 Information Protection in the Health Sector

A security analysis report published by the USA GAO [13] reveals that the USA Department of Health and Human Services (HHS) has initiated actions to identify solutions for protecting personal health information. An overall approach for integrating HHS systems with various privacy related initiatives and for addressing security has not yet been defined. GAO identifies key challenges associated with protecting electronic personal health information in four areas. Two particular areas are relevant to this paper: understanding and resolving legal and policy issues, and implementing adequate security measures for protecting health information. This paper proposes a viable approach which provides the potential for sustainable security measures to protect the privacy and security of health information under an overall trusted health informatics scheme.

4.5 Health Information System Architectures

A modern HIS architecture would normally consist of health application services, middleware, database management system (DBMS), data network control system, operating system and hardware, as shown as in Table 5 (c). Many application users wrongly believe that they have sophisticated security at this level since their applications provide role-based access control or equivalent. It should be understood that no matter what security measures are supported at the application level they are only ever going to be superficial to the knowledgeable adversary or malicious insiders. This approach has a significant limitation in that 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 firmware and hardware facilities of the computer on which it operates. Likewise, any other software component set, such as “middleware”, DBMS, network interface structure or “stack”, is constructed above the operating system and so totally depends upon security functions provided by the operating system as well as the robustness of that operating system against attack.

<table>
<tr><th></th><th>(a)OSI Model</th><th>(b)TCP/IP Model</th><th>(c) HIS Architecture</th></tr>
<tr><td rowspan="6">Software System Components</td><td>Application</td><td rowspan="2">Application</td><td rowspan="2">Health service application
Middleware
DBMS</td></tr>
<tr><td>Presentation</td></tr>
<tr><td>Session</td><td>(not present)</td><td rowspan="4">Data network management system
Operating system</td></tr>
<tr><td>Transport</td><td>Transport</td></tr>
<tr><td>Network</td><td>Internetwork</td></tr>
<tr><td>Data Link</td><td rowspan="2">Network Access</td></tr>
<tr><td>Hardware</td><td>Physical</td><td>Hardware</td></tr>
</table>

Table 5: (a) OSI Model, (b) TCP/IP Model and (c) General HIS Architecture

4.6 Open Trusted Health Informatics Scheme (OTHIS)

HIS involves the definition of structures at a number of levels in computer hardware, operating system, data network control system and health service applications. We propose the Open Trusted Health Informatics Scheme (OTHIS) which is aimed at addressing privacy and security requirements in a holistic manner. OTHIS defines privacy and security requirements at each level within the general HIS architecture to ensure the protection of data from both internal and external threats as well as providing conformance of HIS to meet regulatory and legal requirements.

4.6.1 OTHIS Structure

The OSI reference model (ISO 7289-1) (Table 5(a)) is well known and acknowledged as a baseline for categorisation of network communication functions and assessment. In fact, a fully operational system based on the seven-layer OSI model never attained strong market acceptance. The OSI model envisaged management and control facilities existing at each layer but many of the detailed specifications and activities at each layer were never completed. Instead, TCP/IP (Table 5 (b)) is the model used globally for large scale structures in network communications. The TCP/IP model does not exactly match the OSI model (Table 5 (a)), however the processes defined in the OSI model are contained in the TCP/IP layers. Normally HIS are based around distributed network systems, therefore it is entirely appropriate to

relate the general HIS architecture to the OSI model as well as the TCP/IP model (Table 5). Our research aims to relate and describe the roles and functions performed by each module of the OTHIS architecture, and how they fit into the layers of the OSI and TCP/IP models in a healthcare environment.

It should be noted that the OSI model and HIS architecture can also be categorised into software and hardware components. From the point of view of this paper the first group, software system components, will be addressed. The interpretation of the requirements for appropriate levels of data granularity security in healthcare is the basis of this paper and research work performed to date.

4.7 Health Informatics Access Control (HIAC) Model

An operating system is a set of software programs that manages the hardware and software resources of a computer between the Physical layer and the Application layer of the OSI model and also forms a platform for other system software and application software. It is an inherently futile exercise to attempt to build an application requiring high levels of trust in security and privacy when the underlying structure within the computer system is a non-trusted operating system. The trusted application relies totally upon the non-trusted operating system to access low level services. The authors contend that ICT is now sufficiently advanced that a MAC-based electronic healthcare management system is feasible. Our research to date has indicated that current operating system structures need to be updated for HIS needs. The Health Informatics Access Control (HIAC) model within the OTHIS architecture is our approach to overcoming many of the privacy and security issues which have plagued previous attempts at electronic health management systems. HIAC is based on the MAC/RBAC type of operating system which primarily satisfies the requirement for confidentiality of records (this is a major impediment in current and previous systems). The HIS is then developed atop the trusted operating system.

4.7.1 Analysis of HIS Access Parameters

User role	Capability	DAC	RBAC	MAC	HIAC
Clinicians/ office administrator	User access	Access privileges determined and set by ICT system administrator	Access privileges determined and set (normally) by applications or DBMS/OS	Access determined for each system object (e.g. record) as per set policy	As per MAC
Data custodian	Determine access rights	Tells ICT system administrator who can see what	Tells ICT system administrator who has what role	Specify (possibly create) an appropriate profile for each user (or role with RBAC)	Use suitable profiling language to define HIAC parameters
CEO/CIO	Determine policy	Set organisation general policy	Determines types of roles to suit organisation	Define detailed access policy	Defines organisational policy sets and emergency overrides parameters using natural language
ICT system administrator	Set access rights	Directly program who sees what	As per DAC	Upload (possibly create) policy settings determined by CIO	Upload and manage HIAC profiles
Internal adversary (disgruntled employee)	User access	Can access records inappropriately or feed information to external adversary	As per DAC but more restricted access	Access limited to objects (records) as allowed by relevant policy	HIAC profiles limit violations
External adversary (e.g. hacker)	Penetrate to obtain user access and/or set access rights	Uses Trojans/viruses, social engineering or other illicit means to gain total access	As per DAC	Cannot gain overall control: limited to social engineering (e.g. gain user password for individual's user access)	Requires infeasible levels of knowledge and covert access (further limited by dynamic risk protection mechanisms)

Table 6: Analysis of HIS Access Parameters

As indicated in Table 6, the MAC-based system can provide the ability to limit access to only legitimate authorised users. In general, the organisational security policies are defined by the CEO/CIO. Access privileges are determined by the data custodians. The HIAC profiling mechanism allows for the system administrator to configure the organisational access policies defined and determined by the CEO/CIO and

the data custodian. With MAC the access privileges of all users are equally bound by the policy, not set by the discretion of the file/program owners as with DAC. The internal adversary or disgruntled employee will not be able to access health information inappropriately or even through giving unauthorised information to an external adversary. The MAC mechanism can protect the system from malicious or flawed applications which can potentially damage or destroy the system and its information. This can prevent an external adversary penetrating the system by exploiting Trojan horse attacks, viruses, malware, social engineering or other illicit means to gain total access control or to tamper with audit systems.

4.7.2 HIAC Implementation

4.7.2.1 HIAC Platform

For general applications, currently available products that support the MAC principles of trusted operating systems include “Red Hat Enterprise Linux (RHEL) Version 5”, “Fedora Core 6”, and “Sun Microsystems Solaris 10 with Trusted Extensions Software”. The HIAC model exploits the privacy- and security-enhancement features of such trusted operating systems in the healthcare environment. The end result is a dedicated trusted HIS which satisfies all privacy and security requirements. To determine the practical viability of a HIAC model for HIS a proof-of-concept prototype, based on the Security Enhanced Linux (SELinux) operating system with both the MAC and RBAC approaches, was created [14]. SELinux is based on a flexible, fine-grained MAC architecture named Flask [15]. The HIAC model is necessarily MAC-based accompanied by RBAC properties for flexibility and a refined level of granularity. This degree of simultaneous control and flexibility is not achievable with DAC, RBAC or MAC individually.

4.7.2.2 Protection of Health Service Application Data from the Operating System Level

Redhat’s SELinux enforces domain separation by ‘sandboxes’ known as protected zones to prevent processes and applications interfering with each other, such that an unauthorised process cannot gain overall control of the

system as with DAC. For example, a sandbox in the application level can be created to protect health service applications accessing health data isolated from another sandbox for general activities allowing a Web browser to access the Internet. Unless explicitly permitted, the Web browser is not allowed to access the health data, nor is the health service application permitted to explore the Internet as the Web browser. Once an adversary attacks a DAC system through the network and manages to obtain super-user access privileges, the entire system is subverted. With SELinux however the adversary would control only a single sandbox, and would need to launch additional exploits, each of which becomes increasingly infeasible with distance from the network.

4.7.2.3 Creation of SELinux Proxy at the Application Level

A large scale HIS may involve dynamic and frequent changes to the security policies and security servers such as adding/deleting users and applications. Once the request for the change is made, the SELinux policy needs to be modified and the security server is required to be recompiled manually. In order to provide the minimum of disruption to the system operation and avoid creating additional complex interactions between application and operating system level objects, a proxy is suggested. The proxy operates at the application level and is protected in its own sandbox by SELinux. The proxy regulates access by application-level processes to protect data, using its own set of configuration files. This solution can be seen as nested SELinux, whereby the proxy represents a micro-instance of SELinux that deals only with application data. Operating system level processes see only a monolithic object (the proxy) representing application processes, meaning that the number of configuration rules between the two layers is linear rather than exponential.

4.7.2.4 Proxy Operation

The operation of the proxy mirrors the SELinux mechanism. SELinux separates the policy decision-making logic unit from the policy enforcement logic unit, as shown in Figure 4. For example, a subject X requests to

access an object Y in the system. The policy enforcement server unit queries the security server unit for making an access decision. The security server unit makes the access decision based upon Y's security class and X's security attribute from the security policy database. The access decision is made by the security server and is then relayed to the policy enforcement server unit.

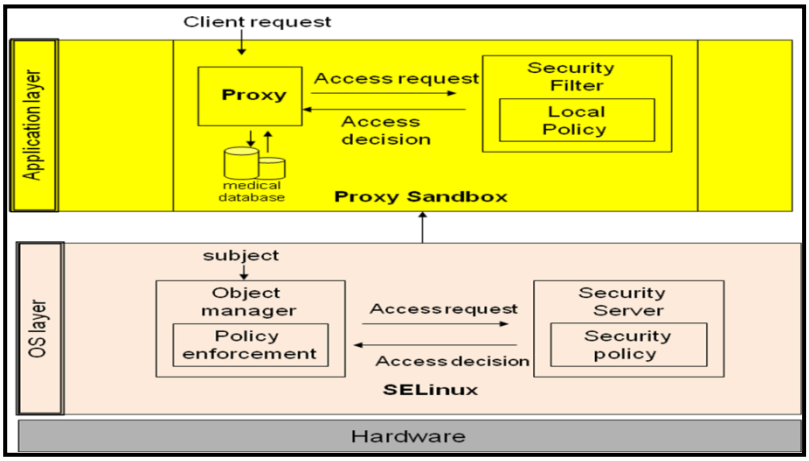


Figure 4: Proxy operation

In the proxy model, a client interacts with the proxy via a pair of Client and Server messages. For each client message received, the proxy sends exactly one server message. In the client message, the client authenticates itself to the proxy with its credentials. Until the next such message is received, the proxy caches the credentials. This mimics the SELinux mechanism, which authenticates a user via a password before transitioning the user into the requested role. The proxy responds to the credentialed message. The credentials are evaluated whenever the client requests access to a record in the proxy database. The proxy passes the credentials with the record identifier and the policy to the security filter. The security filter assesses the credentials, decides whether the record can be accessed in the way intended and passes this decision to the proxy. Whereas SELinux can protect data to the granularity of the file, the proxy has arbitrary granularity, as determined by tags exchanged between the proxy and its client. The client may wish to retrieve a single word from a database, or an entire collection of files. Our mechanism allows this with as little as a single

configuration, although for more complex cases, the number of configuration rules will increase linearly in the number of database items.

There are some cases when records must be accessible even in the absence of legitimate credentials. For example, if the authorised viewer of a patient's case file is not present, but the patient requires emergency treatment, then the availability of the information is more important than its privacy. Thus, the proxy is programmed to respond to a special role of 'Emergency', in which case it moves into auditing mode, until a new set of credentials with a differing role is provided. In auditing mode, all records can be retrieved and modified, but each action is recorded and flagged for review by the security administrator. Appropriate punishment for abusing this mode can be meted out at a social level. Our prototype does not handle differential records, whereby the differences between subsequent versions of records are stored, although this would be advantageous for malicious or accidental modification of records in auditing mode.

Although the proxy significantly simplifies configuration of application data, it does not address problems at the operating-system level that need to be resolved. Further research in this area needs to focus on simplifying the generic SELinux configuration, to allow realistic deployment of "strict" SELinux, which supports protection of application data. This is indeed happening, as witnessed by the development of modular policy logic in Fedora Core 5, which allows the configuration to be developed and loaded in blocks relating to the processes or daemons being protected. The efficacy of this strategy has yet to be solidly determined.

4.7.3 HIAC Features

HIAC incorporates RBAC which complements contemporary MAC systems by ensuring more flexibility over the more traditional MAC standalone systems. In practice this approach gives more flexibility than in the traditional MAC where accesses are granted to individual persons. The proxy model also includes the extended RBAC model with the function of inheritance of permissions with a role hierarchy, so that the policy

configuration can be simplified through the use of role inheritance within hierarchies. The HIAC model includes the principle of least privilege and also enforces domain separation through the use of sandboxes within Redhat's SELinux. These help prevent applications interfering with each other such that an unauthorised user cannot gain overall control of the system as with DAC.

To date Australian privacy laws and health-related privacy legislation prescribe no particular technology to protect personal information. For instance under the Information Privacy Principles (IPP) of the Privacy Act 1988 (Principle 4 – Storage and security of personal information) Principle 4 (a) requires an organisation to take reasonable steps to protect personal information. The National Privacy Principles (NPP) in the Privacy Amendment (Private Sector) Act 2000 also requires a record-keeper to protect personal information by security safeguards as is reasonable. No specific security mechanisms are specified in both the IPP and NPP, thus any reasonable and adequate security measures are allowed for protecting personal information. The HIAC structure enables an effective safeguard strategy for the protection of the confidentiality of individual health information to assist the healthcare industry to comply with Australian privacy legislative and regulatory requirements. Australia's privacy regime is currently under review. This research will continue to observe the update of privacy and e-health privacy legislation in Australia, in order to design the OTHIS architecture for legal compliance.

In general HIAC provides for maximum flexibility within a strongly secure environment. This means that it provides the potential for achieving a balance between security needs and flexibility of implementation, which is primarily determined from a privacy risk assessment. For example HIAC provides the flexibility of having timely access control to assist information resources with an emergency override function by switching to the emergency policy in emergency circumstances. Full auditing of the system deters potential abuses of this flexibility. A major area for future research concerns the simplification of the MAC profile definition. At present the methods and processes needed to define and deploy a mandatory security

policy within an overall HIS are complex and could be considered to be beyond the expertise level of many CIO in health related organisations. Integration of such security profiling structures is required in relation to such other enterprise systems as overall human resource management systems and the like. This allows for definition and deployment of security policies that represent legal, regulatory, policy and enterprise level requirements for reliable and consistent enforcement at the computer system level. This future research requires the definition and implementation of appropriate interfaces between such large scale enterprise systems and the proposed HIAC structure.

4.8 Protection and Enforcement using Cryptography in OTHIS

Cryptographic technologies have long been used for integrity and confidentiality purposes. Large numbers of security-related tools use encryption to protect sensitive information, particularly to maintain privacy. 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 recreate the integrity enforcing checksum, commonly referred as a "message authentication code". 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.

Our research intends to investigate the use of suitable cryptographic techniques embedded into the OTHIS architecture for protecting confidentiality and security of personal health data. Encryption should be used, and normally is used, to protect data in transit for complete end-to-end protection, including within the node systems at each end of a connection. Data in storage should also be encrypted for end-point security against unauthorised or accidental access or eavesdropping. Identity-based encryption mechanisms may be used for identity and/or role management in the healthcare environment. An assessment of suitable cryptographic services and mechanisms for the healthcare sector will be undertaken. Cryptographic integration in the UK, USA and New Zealand healthcare sectors will be investigated. A particularly relevant contribution envisaged from protection and enforcement using cryptography in OTHIS is the elucidation of the requirements for the integration and management of such cryptographic systems in OTHIS for enforcement of privacy and security of electronic health data.

4.9 Conclusion

Our research indicates that an overall trusted HIS should implement security at all levels of its architecture to ensure the protection of personal privacy and security of electronic health information. From an information security perspective, we propose OTHIS for the overall HIS architecture. This paper relates an HIS architecture to two internationally recognised standards, the OSI reference model and the TCP/IP model, to describe how OTHIS fits into these reference models in a HIS. A development of the OTHIS architecture comprises a number of modules with viable and suitable security mechanisms to achieve a high level of security, including the HIAC model. HIAC is a trustworthy access control mechanism to provide the privacy and security of personal health data at the levels of health service application, DBMS, middleware, network control system and operating systems in HIS. HIAC is proposed as a viable solution which has the potential to address the

common types of information privacy violations and weaknesses illustrated by the recent access control management scenarios from Australia, the UK and the USA.

This paper contends that it is both timely and desirable to move electronic HIS towards privacy- and security-aware applications that reside atop a trusted computing-based operating system. Such systems have the real-world potential to satisfy all stakeholder requirements including modern information structures, organisational policies, legislative and regulatory requirements for both healthcare providers and healthcare consumers (privacy and security), and flexible operational demands in HIS. This paper emphasises the need for well-directed research into the application of inherent privacy- and security-enhanced operating systems to provide viable, real-world trusted HIS. The authors propose an HIAC model which has the potential to fulfil these requirements. Future work will be continuing on the development of the other modules within the proposed OTHIS structure with the ultimate goals of maximum sustainability, flexibility, performance, manageability, ease of use and understanding, scalability and legal compliance included in the healthcare environment.

4.10 References

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

[2] J. Quinn, Lessons from the UK EMR: Not Exactly Apples to Apples, 2004. http://www.healthleaders.com/news/print.php?contentid=60316 (accessed 17/08/2005).

[3] D. Sharanahan, P. Karvelas, Welfare workers axed for spying, in The Australian. 2006.

[4] D. Leigh, R. Evans, Warning over privacy of 50m patient files, in Guardian News and Media Limited. 2006.

[5] NHS, "Sealed Envelopes" Briefing Paper Draft, 2005. http://www.ardenhoe.demon.co.uk/privacy/Sealed%20Envelopes%20briefing%20paper.pdf (accessed 03/11/2006).

[6] GAO, Information Security: Department of Health and Human Services Needs to Fully Implement Its Program, 2006. http://www.gao.gov/new.items/d06267.pdf (accessed 12/05/2008).

[7] M. Gasser, Building a Secure Computer System. 1988, New York: Van Nostrand Reinhold.

[8] P. Loscocco, S. Smalley, Integrating Flexible Support for Security Policies into the Linux Operating System, appeared in: Proceedings of the FREENIX Track: 2001 USENIX Annual Technical Conference(FREENIX '01)(2001)
[9] D.F. Ferraiolo, D.R. Kuhn, R. Chandramouli, Role-Based Access Control. 2003, Boston.London: Artech House.
[10] D.E. Bell, L.J. LaPadula, Secure Computer Systems: Mathematical Foundations and Model. 1973, The Mitre Corporation.
[11] J. Reid, I. Cheong, M. Henricksen, J. Smith, A Novel Use of RBAC to Protect Privacy in Distributed Health Care Information Systems, appeared in: Information Security and Privacy, 8th Australasian Conference, ACISP. Wollongong, Australia, (2003)
[12] Microsoft, The Road to Security, 2006. http://www.microsoft.com/resources/ngscb/default.mspx (accessed 28/11/2006).
[13] GAO, Health Information Technology Early Efforts Initiated but Comprehensive Privacy Approach Needed for National Strategy, 2007. http://www.gao.gov/new.items/d07237.pdf (accessed 10/05/2007).
[14] M. Henricksen, W. Caelli, P. Croll, Securing Grid Data Using Mandatory Access Controls, appeared in: 5th Australian Symposium on Grid Computing and e-Research (AusGrid). Ballarat Australia, (2007)
[15] NSA, Security Enhanced Linux, 2000. http://www.nsa.gov/selinux/ (accessed 20/1/2007).

Statement of Contribution of Co-Authors for Thesis by Published Paper

In the case of this chapter:

Publication title: Privacy and Security in Open and Trusted Health Information Systems

Publication status: This paper appeared at the 32nd Australasian Computer Science Conference (ACSC 2009), Wellington, New Zealand. Conferences in Research and Practice in Information Technology (CRPIT), Vol. 97, January 2009.

The authors listed below have certified that:

1. They meet the criteria for authorship in that they have participated in the conception, execution, or interpretation, of at least that part of the publication in their field of expertise;
2. They take public responsibility for their part of the publication, except for the responsible author who accepts overall responsibility for the publication;
3. There are no other authors of the publication according to these criteria;
4. There is no conflicts of interest have been disclosed to (a) granting bodies, (b) the editor or publisher of journals or other publications, and (c) the head of the responsible academic unit, and
5. They agree to the use of the publication in the student's thesis and its publication on the Australasian Digital Thesis database consistent with any limitations set by publisher requirements.

Each author's contributions are listed below:

Contributor	Statement of contribution
Vicky Liu	participated in the conception and design of this manuscript, acquisition of data, analysis and interpretation of the data, writing of this manuscript and acting as the corresponding author
William Caelli	contributed to the conception and design of this manuscript, revising it critically for important intellectual content and final approval of the version to be published
Lauren May	supervised to the conception and design of this manuscript and revising it critically for important intellectual content
Tony Sahama	performed data acquisition on literature review information

Principal Supervisor Confirmation

I have sighted email or other correspondence from all co-authors confirming their certifying authorship.

W CAELLI
Name


Signature

12-8-2010
Date

Chapter 5 Privacy and Security in Open and Trusted Health Information Systems

Vicky Liu, Lauren May, William Caelli and Tony Sahama
Faculty of Information Technology and Information Security Institute
Queensland University of Technology, Australia
PO Box 2434, Brisbane 4001, Queensland Australia
v.liu@qut.edu.au caelli@iisec.com.au l.may@qut.edu.au t.sahama@qut.edu.au

Abstract

The Open and Trusted Health Information Systems (OTHIS) Research Group has formed in response to the health sector's privacy and security requirements for contemporary Health Information Systems (HIS). Due to recent research developments in trusted computing concepts, it is now both timely and desirable to move electronic HIS towards privacy-aware and security-aware applications. We introduce the OTHIS architecture in this paper. This scheme proposes a feasible and sustainable solution to meeting real-world application security demands using commercial off-the-shelf systems and commodity hardware and software products.

Keywords: architecture of health information systems, privacy protection, security for health systems, access control, network security in e-health, application security for health applications

5.1 Background

The OTHIS Research Group at the Information Security Institute (ISI) in the Queensland University of Technology (QUT) has been recently formed in response to industry need for systems expertise in contemporary Health Information Systems (HIS). The Group's vision is to bring together system and network researchers, application domain specialists, and security

specialists to contribute to the design, development and enhancement of a trusted framework for the protection of sensitive health data in HIS. Currently the OTHIS Research Group is chaired by Emeritus Professor William (Bill) Caelli, AO. The Group has already been successful in defining and developing an overall trust architecture based around identification of the separate domains of concern. Preliminary results have been published [1-8].

5.2 Paper Structure

Section 5.3 introduces the concepts of privacy and security in HIS and aligns security requirements for HIS with more general goals and initiatives. The authors' proposal for a secure and open e-health architecture is overviewed in Section 5.4. Sections 5.5, 5.6 and 5.7 discuss the components of this architecture. Future work is outlined in Section 5.8.

5.3 Introduction

As a general principle privacy and security of individual patient data is paramount. In the real world the challenge is to carry this principle through to HIS implementations. The primary goal of the OTHIS Research Group, therefore, is to promote an architecture that provides guidance for technical and security design appropriate to the development and implementation of trusted HIS. This research provides a sufficiently rich set of security controls that satisfy the breadth and depth of security requirements for HIS whilst simultaneously offering guidance to ongoing research projects. In order to meet real-world application security demands that are understandable, implementable and usable, our research themes embrace reasonable security strategies against economic realities using commercial off-the-shelf systems and commodity hardware and software products. Our research team continues to focus on architectural implementation activities around the OTHIS scheme in order to address security requirements at all levels in HIS. The team's future research work will implement and verify the practicality of the OTHIS scheme to a real HIS in partnership with a number of medical institutes.

5.3.1 The Need for Trusted HIS

Social, political and legal imperatives are emerging worldwide for the enhancement of privacy and security in health information systems. A high level of “information assurance” is now accepted as the necessary baseline for the establishment and maintenance of both current and future HIS. A security violation in HIS, such as an unauthorised disclosure or unauthorised alteration of individual health information, has the potential for disaster among healthcare providers and consumers. In a separate paper (Liu et al., 2007) three such real-world scenarios (from Australia, UK and the USA) are identified and analysed from a security and sustainability perspective. Although the concept of Electronic Health Records has much potential for improving the processing of health data, electronic health records may inadvertently pose new threats for compromising sensitive personal health data if not designed and managed effectively. Indeed malevolent motivations could feasibly disclose confidential personal health information on a more widespread scale (potentially massive) and at a higher speed than possible with traditional paper-based medical records. There is also the factor of the healthcare service providers’ willingness to accept and adopt a new technology that does not always facilitate efficient working practices. To encourage healthcare service consumers and providers to use electronic health records, it is crucial to instil confidence that the electronic health information is well protected and that consumers' privacy is assured.

5.3.2 General Health Information Systems

A generic modern HIS architecture normally consists of a number of structures at various levels in computer hardware, firmware, operating system design and facilities, network management system, middleware, database management system and healthcare applications as shown in Figure 5.

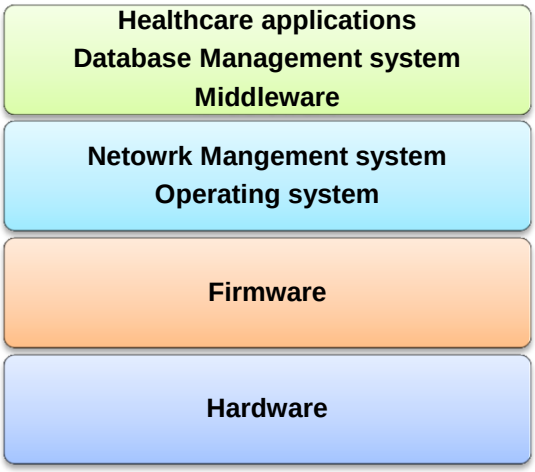


Figure 5: General HIS Structure

Unfortunately, many application users wrongly believe that they have sophisticated security at that particular level since their applications provide a form of message level protection or equivalent. It should be understood that no matter what security measures are supported at the application level they are only ever going to be superficial to the knowledgeable adversary or malicious insider. A significant limitation in this scenario is that the overall application system can be no more secure than the software libraries invoked and incorporated into it, as well as the underlying Web Services upon which the applications depend through such internal actions as systems calls, dynamic library activation, use of intermediate code interpreters such as “JavaScript” or “just-in-time” compilers, etc. The Web Services itself can be no more secure than the firmware and hardware facilities of the computer on which it operates. Likewise, any other software component set, such as “middleware”, database management system, network interface structure or “stack”, is constructed above the Web Services and so totally depends upon security functions provided by the Web Services as well as the robustness of those Web Services against attack. Healthcare applications can be secure and trusted only when the underlying operating system is secure and trusted.

5.3.3 Australian national e-health initiatives

The National E-health Transition Authority (NEHTA) gives direction on developing e-health implementations for the Australian environment. NEHTA

recommends a Service Oriented Architecture and Web Services approach to healthcare application systems [9]. This is recognised as best practice for scalable distributed systems today.

NEHTA work programs for an e-health interoperability framework include Clinical Information, Medicine Product Directory, Supply Chain Efficiency, e-Health Policy, Clinical Terminologies, Individual Healthcare Identifiers, Healthcare Provider Identifiers, Secure Messaging, User Authentication and Shared Electronic Health Record Specifications.

NEHTA focuses on exchanging clinical information by electronic means securely and reliably at the HIS application level. A limitation of this Web Services approach is that security is restricted to the application level only. This is the highest level depicted in Figure 5. Three real-world scenarios, where privacy and security breaches and weaknesses occur external to the application level, are given in Liu et al. (2007). A complete architecture is needed, therefore, and not one that involves just a secure messaging system alone. OTHIS addresses the privacy protection and security for health systems in a holistic and “end-to-end” manner. This incorporates more than just the high-level application layer. The OTHIS architecture also complements existing work already evident in related HIS security areas.

5.4 Proposed Architecture - OTHIS

In order to achieve a high level of information assurance in HIS, we propose a new approach to a more trusted scheme, the Open and Trusted Health Information Systems (OTHIS). The goal of OTHIS is to address privacy and security requirements at each level within a modern HIS architecture to ensure the protection of data from both internal and external threats. OTHIS also has the capability of providing conformance of any HIS to appropriate regulatory and legal requirements. Its primary emphasis in this paper is on the Australian health sector.

5.4.1 OTHIS is an Open Approach

In line with contemporary information technology concepts of open source and open architecture, OTHIS incorporates the term “open”. In order to embrace emerging open architecture, standard and open source technologies are used rather than proprietary technologies. This allows the architecture to be publicly accessible, providing a platform for interoperability. Normally HIS are based around open and distributed network systems. It is therefore entirely appropriate to relate OTHIS to international standards such as Open Systems Interconnection (OSI) security architecture (ISO 7498-2 and ISO/IEO7498-4). This research adopts the broad architectural concepts as proposed in those standards and as adopted for some time by national governments via “Government OSI Profiles”.

5.4.2 OTHIS Builds upon Trusted Systems

Aligned with the concept of trust in information systems, OTHIS also incorporates the term “trusted system”. Any information system depends upon its basic architecture for its general operation. Any trusted information system depends, therefore, upon a trusted base for safe and reliable operation, commonly referred to as a “trusted computing-base”. Without a trusted computing base any system is subject to compromise. In particular, data security at the application level can be assured only when the healthcare application is operating on top of the trusted computing base platform. Threats to the security of healthcare applications can be either externally or internally sourced. In the case of an external threat, an adversary can exploit illicit means to perform actions that bypass or disable the security features of healthcare applications or that grant inappropriate access privileges. In the case of an internal threat, if the HIS is not internally robust authorised users can inadvertently compromise the system. This is a commonplace scenario. Inevitably healthcare applications or databases must be executed upon a trusted platform in order to achieve adequate information assurance. For this reason OTHIS aims at running on top of trusted firmware and hardware bases.

5.4.3 OTHIS is a Modularised Structure

Appropriate data security management involves the protection of data in storage, during processing, and during transmission. The proposed OTHIS structure (Figure 6) addresses all these areas. It consists of three distinct modules:

- Health Informatics Access Control (HIAC),
- Health Informatics Application Security (HIAS), and
- Health Informatics Network Security (HINS).

OTHIS is a modularised architecture for HIS. It is divided into separate and achievable function-based modules. The advantage of the modularisation is that each module is easier to manage and maintain. One module can be changed without affecting the other module. OTHIS is, thus, a broad architecture covering those requirements and parts that may be selected as required to meet particular circumstances. Although there is some overlap across the modules, each module has a specific focus area. HIAC is data-centric dealing with information at rest. HIAS is process-centric dealing with information under processing. HINS is transfer-centric dealing with information under transfer. Trust in network operations through HINS rests completely upon trust in HIAS and HIAC, otherwise the security of messaging becomes futile.

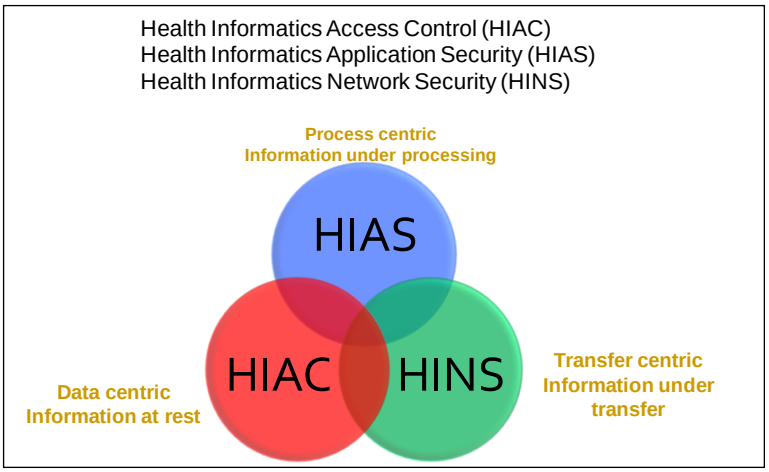


Figure 6: Modularised Structure of OTHIS

5.5 Health Informatics Access Control (HIAC)

“Access control” simply refers to a set of rules that specify which users can access what resources with particular types of access restrictions. Various Web Services, network management systems and database management system can employ a choice of access control mechanisms to grant users access to protected resources of the system. Controlling appropriate access to data in any information system is a major security issue. Many instances of poor access control management practices leading to security and privacy violations are reported on a regular basis [5].

5.5.1 Access Control Models

Discretionary access control essentially assigns responsibility for all security parameters of a data resource to the “owner” (user), usually the data resource creator, who can pass on such parameters to others and perform functions as desired in an unrestricted manner. Role based access control refines the concept to allow for users to be grouped into defined functions or “roles” enabling easier management of overall system security policy particularly in dynamic business environments. Mandatory access control (MAC), in principle, enforces security policy as set out by the overall enterprise and not set up by the data resource “owner”. The traditional MAC policy was originally designed for a military environment. It was based on the multi-level security policy hierarchical structure and was quite rigid in its application. More recent research has modernised the traditional MAC approach to a flexible form of MAC (Flexible MAC) that overcomes traditional MAC limitations. Flexible MAC provides a balance of security needs and flexibility of implementation that allows the security policy to be modified, customised and extended as required in line with normal application and system requirements. The OTHIS/HIAC model is Flexible MAC-based accompanied by Role Based Access Control administration properties for flexibility and a refined level of granularity. This degree of simultaneous control and flexibility is not achievable with Discretionary Access Control, Role Based Access Control or MAC individually.

OTHIS/HIAC proposes a viable solution to provide appropriate levels of secure access control for the protection of sensitive health data. Increasingly, HIS are being developed and deployed based upon commercial, commodity-level information and communications technology products and systems. Such general-purpose systems have been created over the last twenty-five years, often with only minimal security functionality and verification. In particular access control, a vital security function in any Web Services that forms the basis for application packages, has been founded upon earlier designs based on Discretionary Access Control. Discretionary Access Control systems were defined around an environment where data and program resources were developed and deployed within a single enterprise, assuming implicit trust amongst users. This environmental model is no longer valid for modern HIS. In some commercial systems, for example, even the addition of a simple single printer unit has the capacity to seriously undermine the overall integrity of the information system.

5.5.2 Granularity in the HIAC Model

While privacy and security requirements directly relate to identifiable data and information, a far finer level of granularity is needed for security and control management requirements of a real HIS. Not only does HIAC enforce access controls on data files and file directories within the trusted Web Services level, it also provides access control at the {data element, database table}, {row/column}, and cell level views. This can reduce the maintenance cost of managing security at the application level.

5.5.3 Viability of an HIAC model

To determine the practical viability of an HIAC model for HIS a proof-of-concept prototype, based on a “Security Enhanced Linux (SELinux)” computer platform (“Red Hat Enterprise Linux version 4”), was built [3]. This work was carried out at the primitive stage of SELinux project development. As SELinux continues to advance and evolve, our research to date has modernised our HIAC proof-of-concept prototype [10]. Preliminary results of this research indicate that the broad philosophy of Flexible MAC appears

ideally suited to the protection of the healthcare information systems environment.

5.6 Health Informatics Application Security (HIAS)

The overall aim of the OTHIS/HIAS model is to address the data protection requirements at the application level in HIS. HIAS is located at the OSI's "Application Layer", Layer 7, to provide security features which are often required by a healthcare application at a data element level through to a service level. While privacy and security requirements directly relate to identifiable data and information, those HIS elements sitting at higher level information system layers cannot be ignored.

5.6.1 HIAS Legal Compliance

HIAS addresses enterprise policies, and legislative and regulatory requirements, as well as growing social and political demands relevant to the implementation of security controls in HIS with a primary emphasis on the Australian health sector. Based on a Flexible MAC-based concept, OTHIS/HIAS proposes a feasible and reliable solution for the protection of sensitive health data. It satisfies legislative, regulatory and organisational policy requirements for both healthcare providers and healthcare consumers, as well as providing the flexibility to meet operational demands in HIS. This concept is entirely pertinent to the recent e-health privacy blueprint [11] proposed by the Australian Government Office of the Privacy Commissioner, which requests specific enabling legislation in order to protect sensitive health data. Such legislative support is crucial for the proposed national Individual Electronic Health Record systems to be a successful implementation. The objective of the legislation is to gain the trust and confidence of individuals in the Individual Electronic Health Record system.

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 electronic health information is maintained appropriately, and that any such security measures are

understood and accepted by an individual and by society at large. OTHIS/HIAS proposes a Flexible MAC-based scheme for the development of a reliable and sustainable Individual Electronic Health Record system against misuse, disclosure and unauthorised access. This is reinforced by the assertion of the Office of the Privacy Commissioner [11] and NEHTA[33] [12]. They argue that it is necessary to have the "sensitivity label" mechanism in place in the design of a national approach to Individual Electronic Health Record in order to enable individuals and their health providers to have the appropriate level of access they are permitted to have on sensitive health data.

5.6.2 Web Services Security in the HIAS Model

Web Services and Service-Oriented Architecture concepts and implementations are proliferating. The Web Services application model promises to add functional and assessment complexities to the overall information assurance problem by weaving separate components together over the Internet to deliver application services through such methodologies as software "mashups" and the like. These techniques place full trust in the underlying components that are combined into the overall system in a situation where the provenance of those underlying components may not be known.

NEHTA recommends using a Service Oriented Architecture approach to the design of healthcare application systems and the use of "Web Services" as the technology standards for implementing secure messaging systems (NEHTA 2005). NEHTA argues that development of information systems around Web Services technology is the direction in which the information and communications technology industry is heading as well as being accepted as best practice for the design of scalable distributed systems today. The Service Oriented Architecture approach is claimed to lead to more reusable, adaptable and extensible systems over other techniques. In particular, NEHTA supports the concept that Web Services technology has gained

[33]The National E-Health Transition Authority (NEHTA) has been established to accelerate the adoption of e-health by supporting the process of reform in the Australian health sector.

notable attention within the information and communications technology industry and its use is extending in both popularity and market penetration.

The Web Services technology can incorporate security features in the application layer, for example the label “WS-Security” in the header of a “Simple Object Access Protocol” XML message. WS-Security provides a set of mechanisms to maintain finer granular levels of security services such as authentication, confidentiality, integrity and non-repudiation at an element level. For example, WS-security defines how to use XML Encryption and XML Signature processes in the Simple Object Access Protocol to secure message exchanges. Moreover, Web Services is a series of open standards intended to support interoperability in an environment where separate applications need to share information over an open network. As such, any healthcare security architecture must be capable of handling the Web Services paradigm in a trusted, secure and efficient manner.

OTHIS/HIAS also addresses the situation where Web Services structures are being used as the major health informatics information transport methodology. OTHIS recognises that the Service Oriented Architecture approach, implemented through a Web Services structure, has become a major information architecture paradigm. As such, any healthcare security architecture must be capable of handling the Web Services paradigm in a trusted, secure and efficient manner. This, however, provides end-to-end security for data and messages in transit but depends upon an underlying trusted system that supports Flexible MAC principles.

5.6.3 Health Level 7 in the HIAS Model

In developing a trusted system architecture for an HIS, it is important to understand the philosophy of Health Level 7 [13] for medical data transfer. Health Level 7, an American National Standards Institute accredited standard, has been developed to enable disparate healthcare applications to exchange key sets of clinical and administrative data. With respect to the Health Level 7 structure, HIAS depends upon the use of cryptographic subsystems as its security mechanism. Future research programs under

OTHIS will elucidate the relationships between the broad Health Level 7 structure and that of OTHIS from an information assurance perspective. In particular, the focus is on the use of Health Level 7 for both communication and application security and privacy services as needed.

It is necessary to determine which parts of the Health Level 7 standards set belong to either of, or both, HINS and HIAS. The problem of secure messaging structures, however, belongs to the HINS component (as will be described in a forthcoming paper). For example, Health Level 7 requires the use of “digital signatures”. Reliable digital signatures are expected to be created from subsystems within the computer Web Services, and also possibly specific computer hardware under which the HIS works. Without a trusted foundation, the data security of any health applications is inherently vulnerable.

5.7 Health Informatics Network Security (HINS)

HINS consists of the appropriate network level security structure within an underlying HIS. HINS is aimed at the provision of services and mechanisms to authenticate claims of identity, to provide appropriate authorisations (least privileges) following authentication, to prevent unauthorised access to shared health data, to protect the network from attacks, and to provide secure communications health data transmission over the associated data networks. The major function of HINS is the authentication of claimed identities throughout HIS. This includes not only all personnel but also all computing, data storage and computer peripherals such as printers, scanners and network interfaces. OTHIS/HINS involves the vital integration of network security protocols and associated data formats with the access control structures contained within an operating system and allied generic application systems of individual computer nodes.

At the same time the OSI Presentation Layer, as envisaged in the HINS project, will enable cryptographically secured trusted paths to be created between applications at client and server levels in any Service Oriented Architecture environment. The combination of the SELinux/Flexible MAC structures with a clear identification of a new “Layer 6” structure stands at the

centre of the HINS project to enable protection of health systems on an end-to-end basis. Under the HINS scheme, the new Layer 6 will also be managed in the usual way via the creation of essential Flexible MAC user authorisation "profiles" that will be introduced into a running system in a dynamic way in order to be enforced by the new layer. Users will be authenticated into a stated profile at the network level; that is, without connection to any specific health information server host. In this sense, an authenticated user will be able to present an authorisation vector to any allowed host in the approved network in such a way that the separation of such hosts will not be obvious to the end-user.

The OTHIS/HINS project is currently under development. The broad system architecture is nearing completion. The connection of Flexible MAC "compliant" servers and network elements into the overall structure is being defined against stated health information system requirements. Progress so far has demonstrated the basic concept of a "presentation layer" style "stub" structure for use by common application packages.

5.8 Conclusion and Future Work

The concepts of privacy and security in HIS were introduced in Section 5.3 along with the alignment of security requirements for HIS with more general goals and initiatives. Section 5.4 overviewed the authors' proposal for a secure and open e-health architecture. Components of this architecture are further detailed in Sections 5.5, 5.6 and 5.7.

Our research indicates that an overall trusted HIS should implement security at all levels of its architecture to ensure the protection of personal privacy and security of electronic health information. From an information security perspective, we propose OTHIS for the overall HIS architecture. This comprises a set of complementary security architectures consisting of HIAC, HIAS and HINS. This proposed OTHIS scheme will be tested through experimental structures created on trusted Web Services. Key research questions to be answered include those concerning both system efficiency and availability aspects of the proposed architecture. Preliminary results of this research indicate that the broad philosophy of Flexible MAC appears

ideally suited to the protection of the healthcare information systems environment.

We contend that it is both timely and desirable to move electronic HIS towards privacy-aware and security-aware applications that reside atop a trusted computing-based Web Services. Such systems have the real-world potential to satisfy all stakeholder requirements including modern information structures, organisational policies, legislative and regulatory requirements for both healthcare providers and healthcare consumers (privacy and security), and flexible operational demands in HIS. This paper emphasises the need for well-directed research into the application of inherent privacy- and security-enhanced operating systems to provide viable, real-world trusted HIS. The OTHIS scheme has the potential to fulfil these requirements. Future work continues on the development of the other modules within the proposed OTHIS structure with the ultimate goals of maximum sustainability, flexibility, performance, manageability, ease-of-use and understanding, scalability and legal compliance in the healthcare environment.

5.9 References

[1] P. Croll, M. Henricksen, W. Caelli, V. Liu, Utilizing SELinux to Mandate Ultra-secure Access Control of Medical Records, appeared in: 12th World Congress on Health (Medical) Informatics, Medinfo2007. Brisbane Australia, (2007)

[2] L. Franco, T. Sahama, P. Croll, Security Enhanced Linux to Enforce Mandatory Access Control in Health Information Systems, in: Australasian Workshop on Health Data and Knowledge Management, the Australian Computer Science Week. Wollongong, Australia: ACM (2008).

[3] M. Henricksen, W. Caelli, P. Croll, Securing Grid Data Using Mandatory Access Controls, appeared in: 5th Australian Symposium on Grid Computing and e-Research (AusGrid). Ballarat Australia, (2007)

[4] V. Liu, W. Caelli, L. May, Strengthening Legal Compliance for Privacy in Electronic Health Information Systems: A Review and Analysis, in: National e-Health Privacy and Security Symposium, ehPASS'06. Queensland University of Technology, Brisbane, Australia (2006).

[5] V. Liu, W. Caelli, L. May, P. Croll, A Sustainable Approach to Security and Privacy in Health Information Systems, appeared in: 18th Australasian Conference on Information Systems (ACIS) Toowoomba, Australia, (2007)

[6] V. Liu, W. Caelli, L. May, P. Croll, Strengthening Legal Compliance for Privacy in Electronic Health Information Systems: A Review and

Analysis. The Electronic Journal of Health Informatics (eJHI), 2008. Vol 3 (1: e3).

[7] V. Liu, W. Caelli, L. May, P. Croll, Open Trusted Health Informatics Structure, in: Australasian Workshop on Health Data and Knowledge Management, the Australian Computer Science Week Wollongong Australia: ACM (2008).

[8] V. Liu, W. Caelli, L. May, P. Croll, M. Henricksen, Current Approaches to Secure Health Information Systems are Not Sustainable: an Analysis, in: 12th World Congress on Health (Medical) Informatics, Medinfo. Brisbane, Australia (2007).

[9] NEHTA, Towards an Interoperability Framework. 2005, National E-health Transition Authority.

[10] L. Martin Franco, SELinux Policy Management Framework for HIS (under examination) in Faculty of Information Technology. 2008, Queensland University of Technology: Brisbane, Australian.

[11] Australian Government Office of the Privacy Commissioner, Consultation on the Privacy Blueprint for the Individual Electronic Health Record, 2008. http://www.privacy.gov.au/publications/sub_nehta_0808.pdf (accessed 2/09/2008).

[12] NEHTA, Privacy Blueprint for the Individual Electronic Health Record, 2008. http://www.nehta.gov.au/index.php?option=com_docman&task=cat_view&gid=-2&Itemid=139 (accessed 10/08/2008).

[13] Health Level Seven Study Guide. 2008: OTech.

Statement of Contribution of Co-Authors for Thesis by Published Paper

In the case of this chapter:

Publication title: Open and Trusted Information Systems/Health Information Access Control (OTHIS/HIAC)

Publication status: This paper appeared at the 32nd Australasian Computer Science Conference (ACSC2009), Wellington, New Zealand. Conferences in Research and Practice in Information Technology (CRPIT), Vol. 98, January 2009

The authors listed below have certified that:

1. They meet the criteria for authorship in that they have participated in the conception, execution, or interpretation, of at least that part of the publication in their field of expertise;
2. They take public responsibility for their part of the publication, except for the responsible author who accepts overall responsibility for the publication;
3. There are no other authors of the publication according to these criteria;
4. There is no conflicts of interest have been disclosed to (a) granting bodies, (b) the editor or publisher of journals or other publications, and (c) the head of the responsible academic unit, and
5. They agree to the use of the publication in the student's thesis and its publication on the Australasian Digital Thesis database consistent with any limitations set by publisher requirements.

Each author's contributions are listed below:

Contributor	Statement of contribution
Vicky Liu	participated in the conception and design of this manuscript, acquisition of data, analysis and interpretation of the data, writing of this manuscript and acting as the corresponding author
Luis Franco	performed data acquisition on a proof of concept application development for the proposed OTHIS/HIAC architecture
William Caelli	contributed to the conception and design of this manuscript, revising it critically for important intellectual content and final approval of the version to be published
Lauren May	supervised to the conception and design of this manuscript and revising it critically for important intellectual content
Tony Sahama	performed data acquisition on literature review information

Principal Supervisor Confirmation

I have sighted email or other correspondence from all co-authors confirming their certifying authorship.

W CAELLI
Name

Signature

12-8-2010
Date

Chapter 6 Open and Trusted Information Systems/Health Informatics Access Control (OTHIS/HIAC)

Vicky Liu, Luis Franco, William Caelli, Lauren May, and Tony Sahama
Faculty of Information Technology and Information Security Institute
Queensland University of Technology, Australia
PO Box 2434, Brisbane 4001, Queensland Australia
{v.liu, luis.franco, w.caelli, l.may, t.sahama}@qut.edu.au

Abstract

Information and Communications Technologies globally are moving towards Service Oriented Architectures and Web Services. The healthcare environment is rapidly moving to the use of Service Oriented Architecture/Web Services systems interconnected via this global open Internet. Such moves present major challenges where these structures are not based on highly trusted operating systems. This paper argues the need of a radical re-think of access control in the contemporary healthcare environment in light of modern information system structures, legislative and regulatory requirements, and security operation demands in Health Information Systems. This paper proposes the Open and Trusted Health Information Systems (OTHIS), a viable solution including override capability to the provision of appropriate levels of secure access control for the protection of sensitive health data.

Keywords: access control, architecture of health information systems, security for health information systems, health informatics, information assurance, trusted system, open solutions

6.1 Introduction

Social, political and legal imperatives are emerging worldwide for the enhancement of the privacy and security of health information systems (HIS). A high level of “information assurance” is now seen as the necessary baseline for the establishment and maintenance of both future and current HIS. A security violation in HIS, such as an unauthorised disclosure or unauthorised alteration of individual health information, has the potential for disaster among healthcare providers and consumers.

Indeed, such emerging legal obligations as “breach notification”, whereby custodians of private data are legally compelled to divulge any real or suspected breach in privacy to possible victims, are gaining international attention. This has been recently referenced by the USA legal firm, Steptoe & Johnson LLP [1] , in the following terms:

> *New data protection requirements are being considered all over, including in Australia, Mexico, Turkey, South Korea, Peru, and Vietnam.*

Although the concept of Electronic Health Records has much potential for improving the processing of health data, electronic health records may also pose new threats for compromising sensitive personal health data if not designed and managed effectively. Indeed malevolent motivations could feasibly disclose confidential personal health information on a more massive scale and at a higher speed than possible with traditional paper-based medical records. There is also the factor of the healthcare service providers’ willingness to accept and adopt a new technology that does not always facilitate efficient working practices. To encourage healthcare service consumers and providers to use electronic health records, it is crucial to instil confidence that the electronic health information is well protected and that consumers' privacy is assured. Indeed, unlike other industries and enterprises such as the banking and finance sectors, loss and disclosure of health record data is normally not recoverable. Again unlike the banking sector, a new “account” cannot be created along with all other necessary identification and authentication data and processes. Health data is usually “locked” to an individual.

However, it can be argued that concepts of privacy, with resulting requirements placed on data holders to maintain associated confidentiality, have rapidly changed in part due to the widespread acceptance of Internet based “social networking” and the very low cost of Terabyte level data storage facilities. Indeed Dyson [2] has proposed that, in an era of “*Facebook*”, “*Flickr*” and associated systems and services for “free” data sharing, the concept of individual privacy may be rapidly changing. This change involves a move from closely guarding the confidentiality of personal data records to one of personal control over access to that data. Dyson states that “…people are learning to exert some control over which of their data others can see...”. Dyson continues to point out that such control over access must become more dynamic and even allow for certain levels of ambiguity in just how such access patterns may be defined and managed by individuals, particularly as this relates to health records. Moreover, such access control structures have to be “user friendly”, allowing those non-expert in aspects of information and data communications technology to understand and administer associated computer based systems.

6.1.1 Security Requirements for E-health

Achieving the usual security goals, normally applied through confidentiality, integrity and availability constraints, for HIS is an essential requirement and not just a technology feature. Privacy concerns take on new importance in this environment and may, in some cases, modify aspects of the usual confidentiality-integrity-availability trilogy. At the same time, emergency override requirements may involve more complex definition and implementation of confidentiality schemes. This can involve further parameters of time and location, identity and authentication when accessing healthcare, law enforcement or allied professionals, etc. Security techniques are a critical factor in the successful implementation of e-health initiatives. Several countries such as Australia, the United Kingdom (UK) and the United States of America (USA) are actively involved in the development of national e-health initiatives. These designs rely upon a basic set of security requirements to implement their e-health initiatives.

The USA government intends to reform its national healthcare system with the goal of improving the effectiveness and efficiency of healthcare operations whilst assuring that sensitive health information remains private and secure through their 1996 Health Insurance Portability and Accountability Act (HIPAA). The purpose of HIPAA provisions is to encourage electronic transactions whilst simultaneously requiring appropriate security measures for protection of the individually identifiable health information.

Australia's National E-health Transition Authority[35] (NEHTA) clearly defines similar security goals in its mission statements. They emphasise the importance of creating a complete, usable and implementable security architecture for HIS. NEHTA also recognises that privacy perceptions of the Australian community play a major role in ensuring the success of e-health systems.

In the case of the UK, the National Health Service (NHS) also clearly affirms the principles of information security[36] to require that all reasonable safeguards are in place to prevent inappropriate access, unauthorised modification or manipulation of sensitive patient record information.

Section 6.2 discusses the related work undertaken by the Australian national e-health body, National E-health Transition Authority (NEHTA). The Open and Trusted Health Information Systems (OTHIS) structure is our approach to providing a viable e-health system with the potential for implementing sustainable security measures. OTHIS, outlined in Section 6.3, has the capacity to protect the privacy and security of health information under an overall trusted health informatics scheme. This paper focuses on one of the OTHIS modules, Health Informatics Access Control (HIAC), in Section 6.4. An analysis of HIAC is presented in Section 6.5. Finally, conclusions are drawn and future directions for OTHIS are discussed in Section 6.6.

[35] NEHTA was established by Australia's Federal Government in 2005 to oversee the introduction of a system of national electronic health records. Its statement of mission is available at http://www.nehta.gov.au/ accessed 12/07/2008.
[36] The principles of information security from UK NHS are available http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/security accessed 12/07/2008.

6.2 Related Work

An analysis of common existing approaches to secure health information systems in Australia, UK and the USA is given by Liu, Caelli, May and Croll (2007). In this paper which addresses sustainability of HIS systems, three scenarios related to information privacy violations and weaknesses are identified and discussed. As we are concerned with e-health infrastructures that satisfy the Australian environment, Section 6.2.1 discusses the Australian direction on this given by NEHTA. Section 6.2.2 discusses the NEHTA approach from the authors' perspectives.

6.2.1 National E-health Transition Authority

NEHTA recommends using a Service Oriented Architecture approach to the design of healthcare application systems. "Web Services" technology standards provide the capacity for implementing secure messaging systems [3]. NEHTA argues that the continued development of information systems around Web Services technology is leading the way for the information and communications technology industry into its realisation of this Service Oriented Architecture approach. Web Services are also accepted as best practice for the design of scalable distributed systems today. The Service Oriented Architecture approach is claimed to lead to more reusable, adaptable and extensible systems over other techniques. In particular, NEHTA supports the concept that Web Services technology has gained notable attention within the information and communications technology industry. Its use is extending in both popularity and market penetration.

NEHTA work programs for an e-health interoperability framework include Clinical Information, Medicine Product Directory, Supply Chain Efficiency, e-Health Policy, Clinical Terminologies, Individual Healthcare Identifiers, Healthcare Provider Identifiers, Secure Messaging, User Authentication and Shared Electronic Health Record Specifications.

6.2.2 Discussion on NEHTA Approach

NEHTA focuses on exchanging clinical information by electronic means securely and reliably. This may be achievable at the data communications link level by using secure messaging technology. The fact is however that the associated and critical health information computer systems will be openly connected to the Internet, and thus be exposed to “cyber-attacks”. This exposure has not been prevalent before. In this Internet connectivity environment, the issues of data “at rest” and “under processing” within a specific operating system are far more critical, as is evidenced by any cursory examination of illicit penetration of computer systems connected to the Internet globally. A complete architecture is needed, therefore, and not one that involves just a secure messaging system alone. OTHIS addresses the privacy protection and security for health systems in a holistic and “end-to-end” manner. The OTHIS architecture is designed to complement existing work already evident in related HIS security areas.

6.3 Our Approach – Open and Trusted Health Information Systems (OTHIS)

Security may be implemented at the level of the health services applications system. Even if security is established within that health service system, however, 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 at the higher levels is totally dependent upon the security functions provided at the lower levels. Examples of such software include “middleware”, database management systems, the network interface structure, and the “stack”. The lowest level software is the operating system which provides the foundational security for the higher levels. The operating system also needs a degree of “robustness” against possible attacks at its level.

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. 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, Smalley, Muckelbauer, Taylor, Turner and Farrell [4] 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.

Our approach caters for the trusted operating system with the capacity to provide a viable and sustainable solution for the protection of sensitive health data in the healthcare environment. The authors define the characteristic features of OTHIS as:

- OTHIS is an holistic approach to HIS consistent with health legal requirements,
- OTHIS is an open architecture,
- the OTHIS scheme builds on the top of trusted firmware and hardware bases, and
- OTHIS is modularised architecture.

6.3.1 Holistic Approach to HIS

In achieving a high level of information assurance in HIS, we propose an holistic approach to a more trusted scheme, the Open and Trusted Health

Information Systems (OTHIS). The goal of OTHIS is to address privacy and security requirements at each level within a modern HIS architecture to ensure the protection of data from both internal and external threats. OTHIS has the capacity to ensure legal compliance of any HIS to appropriate legislative and regulatory requirements. The primary emphasis in this paper is on the Australian health sector.

6.3.2 Open Architecture

OTHIS takes an open approach that can provide cost effective, viable and sustainable architecture to security and privacy in HIS. OTHIS embraces emerging open architecture, standard and solution technologies rather than use proprietary technologies. The inclusion of “open” in the OTHIS framework is to allow our proposed architecture to be available for public access and to provide a platform for interoperability. This approach is also supported by Goldstein Groen, Ponkshe and Wine [5]. Open systems allow disparate HIS to communicate and exchange clinical information in an open network environment. Normally HIS are based around open and distributed network systems; therefore, it is entirely appropriate to relate OTHIS to international standards such as Open Systems Interconnection (OSI) security architecture through standards ISO 7498-2 and ISO/IEO7498-4. This research adopts the broad architectural concepts as proposed in those standards and as adopted for some time by national governments via “Government OSI Profiles”.

6.3.3 Trusted Platform

OTHIS also involves the term “trust”, relating to “trusted system”. Any information system depends, fundamentally, upon a trusted base for safe and reliable operation, commonly referred to as a “trusted computing-base”. Without a trusted computing-base any system is subject to compromise. In particular, data security at the application level can be assured only when the healthcare application is operating on the top of the trusted computing-base platform. Otherwise the adversary can exploit illicit means to perform the actions that bypass or disable the security features of healthcare applications

or that grant inappropriate access privileges. Inevitably healthcare applications or databases must be executed atop the trusted platform in order to achieve adequate information assurance. For this reason OTHIS aims at running on the top of trusted firmware and hardware bases. This trusted firmware and hardware base is commonly referred to as a Trusted Platform Module. This research assumes a commodity Trusted Platform Module upon which to deploy OTHIS. Many such modules are available in the marketplace.

6.3.4 Modularised Architecture

Appropriate data security management involves the protection of such data in storage, during processing and transmission. The proposed OTHIS structure (Figure 7) addresses all these areas and consists of three of distinct modules:

- Health Informatics Access Control (HIAC),
- Health Informatics Application Security (HIAS), and
- Health Informatics Network Security (HINS).

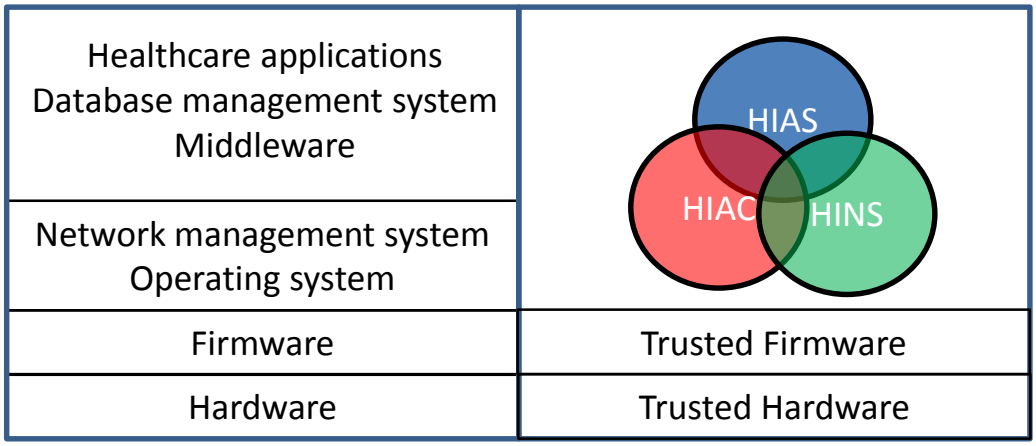


Figure 7: Open and Trusted Health Information Systems

OTHIS is a modularised architecture for HIS. It can be clearly divided into separate and achievable function-based modules. The advantages of the modularisation include the fact that each module is easier to manage and maintain. One module can be changed without affecting the other module. OTHIS is, thus, a broad architecture covering those requirements and parts

that may be selected as required to meet particular circumstances. There is some overlap with these three modules; however, each module has a specific focus area. HIAC is data centric dealing with information at rest, HIAS is process centric dealing with information under processing, and HINS is transfer centric dealing with information under transfer. Trust in network operations through HINS rests completely upon trust in HIAS and HIAC; otherwise the security of messaging becomes futile. The focus of this paper is on the HIAC model.

6.4 Health Informatics Access Control (HIAC)

Access control mechanisms are used to define and then restrict users' access to resources. Organisations would normally use these controls to grant employees, for example, the authority to access only the information those users need to perform their duties, i.e. the principle of "least privilege". Access controls can limit the activities that an employee can perform on data at the level of granularity desired. Access control mechanisms are therefore enabled at the operating system level as well as higher levels including data network management and the database management systems for the application.

Access control is one of the fundamental security mechanisms used to protect computer resources, in particular in multi-user and resource-sharing computer based environments such as those incorporated into a contemporary HIS. The lack of adequate access control and associated system management in health relevant computer systems has been demonstrated on numerous occasions in recent history, including the privacy invasion situation at Australia's Centrelink [6], the lack of adequate safeguards in the UK NHS patient records system [7], and the significant information technology security weaknesses identified in the US HHS information system [8]. These types of information privacy violations or weaknesses have the potential for inflicting, and do inflict, major harm on HIS consumers and providers alike. The issue of providing suitable computer operating system access control in such systems is not an insurmountable

one. Indeed, appropriate computer-based access control schemes do exist and can be deployed to address these information security issues.

6.4.1 Access Control Models

Discretionary access control essentially assigns responsibility for all security parameters to the “owners” (users) of such larger entities, usually their creator, who could pass on such parameters to others and perform functions as desired. Role-based Access Control refines the concept to allow users to be grouped into defined functions or “roles” allowing for far easier management of overall system security policy particularly in dynamic business environments. Mandatory access control (MAC), in principle, enforces security policy as set out by the overall enterprise and not set up by definitions provided by file/program “owners”. The traditional MAC policy was originally designed for a military environment based on the multi-level security policy hierarchical structure and was quite rigid in its application. More recent research has modernised the traditional MAC approach to a flexible form of MAC (Flexible MAC) that overcomes traditional MAC limitations with the enforcement of a wider range of security requirements including confidentiality, integrity, least privilege and separation of duty.

6.4.2 HIAC is Flexible MAC-based Architecture

HIAC is a Flexible MAC-based model accompanied by Role-based Access Control properties to simplify authorisation management. This degree of simultaneous control, flexibility and a refined level of granularity is not achievable with Discretionary Access Control, Role-based Access Control or MAC individually. HIAC proposes a viable solution to providing appropriate levels of secure access control for the protection of sensitive health data. Increasingly, HIS are being developed and deployed based upon commercial, commodity-level information and communications technology products and systems. Such general-purpose systems have been created over the last 25 years with often only minimal security functionality and verification. In particular access control, a vital security function in any operating system that forms the basis for application packages, has been

founded upon earlier designs based on Discretionary Access Control. Discretionary Access Control systems were defined around an environment where data and program resources were developed and deployed within a single enterprise, assuming implicit trust amongst users. This environmental model is no longer valid for modern HIS. In some commercial systems, for example, even the addition of a simple single printer unit has the capacity to seriously undermine the overall integrity of the information system.

6.4.3 HIAC Platform

Currently available products that support the MAC principles of operating systems include:

- “Red Hat Enterprise Linux (RHEL) Version 5 and “Fedora Core 9”,
- “Sun Microsystems Solaris 10 with Trusted Extensions Software”,
- “Novell SUSE Linux Application Armor (AppArmor)”, and
- “FreeBSD 5.0”.

The HIAC model exploits the security-enhancement features of such trusted operating system in the healthcare environment. The end result is a dedicated trusted HIS which satisfies all security requirements. To determine the practical viability of a HIAC model for HIS a proof-of-concept prototype was built on the Security Enhanced Linux (SELinux) operating system by Henricksen, Caelli and Croll. [9] with RHEL Version 4. This was later modernized by Franco Martin [10] with Fedora Core 9.

6.4.4 Flask Architecture – Flexible MAC – SELinux

The U.S. National Security Agency designed and engineered SELinux with a security architecture named the Flux Advanced Security Kernel (Flask). It aims to set an example of how Flexible MAC could be added to a mainstream operating system to greatly improve the security of the system. Flexible MAC provides a balance of security needs and flexibility of implementation that allows the security policy to be modified, customised and extended as required in line with normal application and system requirements. SELinux also provides separation of security domains as a

fail-safe feature to enable the confinement of damage caused by the probability of malicious or flawed code execution [11]. The flexibility of SELinux includes the separation of the security policy logic from the enforcement mechanism. This enables the independent policy module to be modified and extended as required without affecting the rest of the kernel or the need to restart the system.

6.4.5 Protection and Enforcement Using SELinux Policy and Profile in HIAC

In general, the organisational security policies are defined by CEO/CIO. Access privileges are determined by the data custodians. The system administrator configures and deploys the organisational access policy defined and determined by the CEO/CIO and the data custodian. The following sections describe the procedures of developing a security policy and using SELinux security mechanisms to protect sensitive health information for HIS.

To use SELinux Policy to implement the organisational access policy, one must understand the SELinux Policy mechanisms. SELinux Policy is a collection of rules that determine allowed access for a system created in accordance with the corporate security policy. An SELinux Policy consists of a set of SELinux Profiles (policy modules) that define the associated security properties controlling the security behaviour of the system. The following procedure steps show the development of an SELinux policy (Figure 8):

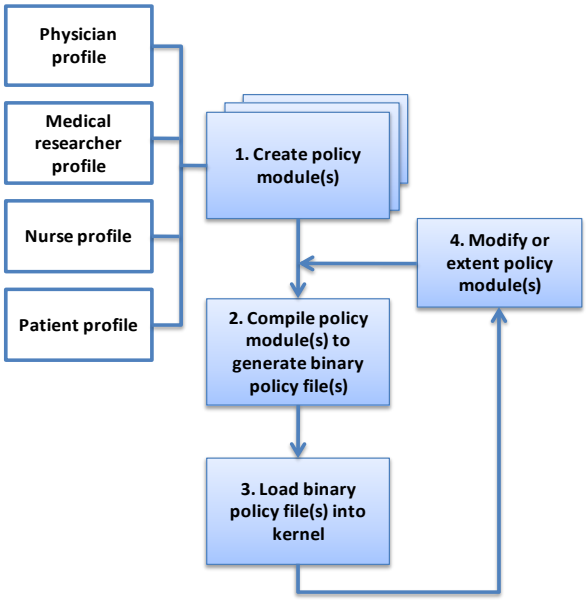


Figure 8: SELinux Profile Development Cycle

1. Create policy module(s), such as for physicians, medical researchers, nurses and patients policy modules.
2. Compile the policy module(s) to generate the binary policy file(s) as a loadable kernel module(s).
3. Load the binary policy file(s) into the running kernel for access enforcement.
4. If policy module(s) require(s) changes, the modified policy module(s) is (are) recompiled and then reloaded into the running kernel.

6.4.6 SELinux Concepts – User Identifier, Role and Type Identifier

The SELinux Policy is now configured and loaded into the kernel ready for operation. Figure 9 shows the authorisation process flow in SELinux.

Figure 9: Authorisation Process Flow in SELinux

After a user is authenticated to the SELinux system, the user logs into the system with his/her username which is associated with a Linux unique user identifier (UID). A Linux UID is generated when a user account is created (Table 7). A user may have more than one user account. In SELinux, the

system administrator maps the Linux UID(s) of the user to an SELinux UID, so that any action performed within the system by the same user can be traced for accountability. In addition, having different user identifiers helps to keep Linux Discretionary Access Control mechanisms separated from the SELinux MAC mechanisms.

The user access privileges, which are user, role, domains and types associated with SELinux UID, are defined in the SELinux Policy. The system verifies the SELinux Policy to retrieve access privileges which define the SELinux Profile of the user. The authorised access can now begin from this point.

SELinux Profile	Linux UID	SELinux UID	Role	Authorised Domain
Physician	drpaul (501)	hc_doc_u	hc_doc_r	hc_doc_diag_t
Medical Researcher	resjohn (502)	hc_res_u	hc_res_r	hc_res_diag_t
Nurse	nuralice (503)	hc_nur_u	hc_nur_r	hc_nur_diag_t
Patient	patluis (504)	hc_pat_u	hc_pat_r	hc_pat_diag_t

Table 7: Linux UID, SELinux UID, Role and Type

6.4.7 SELinux Security Mechanisms to Protect Sensitive Health Data

In SELinux, Type Enforcement (TE) is the basis for the primary access control feature where such an access control structure is based on security contexts. All subjects and objects have a type identifier associated with them. To access an object, the subject's type must be authorised for the object's type. Namely, TE makes access decisions based on security contexts to determine access. A security context consists of three elements: user, role and type identifier.

With SELinux, users are assigned a set of roles which determine a set of processes authorised for the user's identity. Domains are used to specify how roles can interact with subjects and objects in the system. Different sets of domains are authorised for each of the user roles based on the TE rules defined in the SELinux policy.

SELinux allows dividing the system space into a set of “sandboxes” determined by the authorised user domains. An application running on behalf of a user is allowed to access certain resources in the system. To prevent unauthorised access, a medical related sandbox can be used to isolate a space in which a medical application is permitted to access medical records. The following clinical scenario is used to explain this concept.

It is assumed that a doctor “Paul” is associated with a physician role, which is allowed to run the Diagnostic Application within a specified domain “hc_doc_diag_t” and is allowed to access the files with type “hc_diag_file_t”. In fact, when Paul activates the Diagnostic Application, the system process labelled with the domain “hc_doc_diag_t”, is acting on behalf of Paul. It enters the domain “hc_diag_doc_t” with specified access permissions to the those objects and subject types associated with this domain only. Assume that user “John” is associated with a medical researcher role. Even if John is allowed to access the Diagnostic Application, John is accessing this application through the domain “hc_res_diag_t”. This domain is authorised to access different resources than the physician. Therefore, even if they use the same application, in the same system, they cannot access the same resources.

SELinux Sandboxes can be constructed to protect medical data from a compromised application (Figure 10).

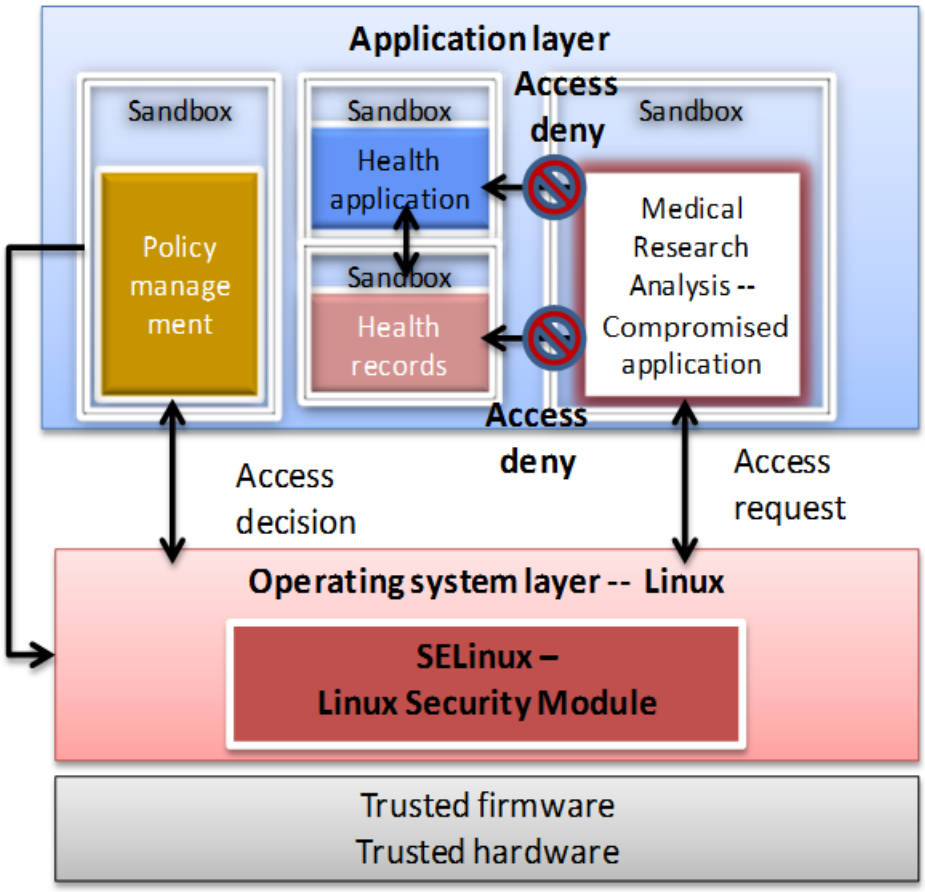


Figure 10: Protect Sensitive Health Data with SELinux

Medical researchers are authorised to access the medical information for secondary usage within another sandbox. If a “backdoor” is open for a hacker to gain access privileges over unauthorised resources, the hacker only has access to the medical information for secondary usage within that sandbox. The damage from this compromised application therefore can be contained within a single domain, not the entire system. In contrast, in a Discretionary Access Control based system, the damage from compromised applications cannot be restricted within a space. In particular, if the hacker gains the access privileges of a system administrator, the entire system is compromised including the sensitive individual health information.

6.4.8 Example of an SELinux Policy Module

This section provides an example of coding for SELinux Profile in relation to how a physician and a medical researcher can run the Diagnostic Application with different accesses to different types of health data files. The two users

can be defined in SELinux: “hc_doc_u” and “hc_res_u”. The code specifies the sandboxes to be accessed when the authorised physicians and medical researchers run the Diagnostic Application, that is “hc_doc_diag_t” for the authorised physicians and “hc_res_diag_t” for the authorised medical researchers. The domain “hc_res_diag_t” is configured in the policy module to allow access the data files with type “hc_res_dbfile_t” (i.e. data files for the authorised researchers accesses). The domain “hc_doc_diag_t” is specified to access the data files with type “hc_pnt_dbfile_t” (i.e. sensitive health data files). In such a way, the medical researcher is not able to access sensitive data files with the unauthorised role. That is, the medical researcher can access only the domain “hc_diag_res_t” and data files associated with type “hc_res_dbfile_t”.

```
# Type for the Diagnostic Application executable file

type hc_diag_sys_exec_t;

files_type(hc_diag_sys_exec_t)

# Type for the DB files which can be accessed by researchers.

Type hc_res_dbfile_t;

files_type(hc_res_dbfile_t)

# Type for the DB files which can be accessed by physicians.

# This type can be assigned to files containing sensitive information.

Type hc_pnt_dbfile_di_t;

files_type(hc_pnt_dbfile_di_t)

# This interface creates types, roles and domains to be assigned to physicians.
```

```
Healthcare_create_users(hc_doc)

# This interface creates types, roles and domains to be assigned to

#  researchers.

Healthcare_create_users(hc_res)

# These interfaces assign only the necessary privileges for the user to access

# their home directory.

# This interface authorises physicians to access the delegated sandbox while

# executing the Diagnostic Application.

Diag_general_domain(hc_doc)

# This authorises researchers to access the delegated sandbox during

# executing the Diagnostic Application.

Diag_general_domain(hc_res)

# The “diag_general_domain” is described in more detail further in this document.

# These references to this interface create two domains which constitute the

# sandboxes for physicians and researchers: hc_doc_diag_t and hc_res_diag_t.

# This line of code authorises physicians to create, write and read DB files

# with the type hc_pnt_dbfile_di_t while operating within the boundaries of the

# sandbox. The boundary of the sandbox is defined with the domain

# hc_doc_diag_t.

allow hc_doc_diag_t hc_pnt_dbfile_di_t:file { create_file_perms \

                    write_file_perms read_file_perms };
```

```
# This line of code authorises researchers to create DB files with the type

# hc_res_dbfile_di_t while operating within the boundary of the delegated
#sandbox.

# The boundaries of the sandbox are defined with the domain hc_res_diag_t.

allow hc_res_diag_t hc_res_dbfile_di_t:file { read_file_perms };

# The following 2 statements authorise the roles corresponding to physicians

# and researchers to access their corresponding domains.

role hc_doc_r types { hc_doc_diag_t };

role hc_res_r types { hc_res_diag_t };
```

An SELinux Policy is comprised of different components. These components can be placed in three different files: type enforcement, context file and interface files. In the above code, researchers and physicians are authorised to access their delegated specific sandboxes while running the Diagnostic Application. These privileges are granted through the use of the "diag_general_domain" interface which is shown below.

```
interface('diag_general_domain',`

  type $1_diag_t;

  domain_type($1_diag_t)

  domain_auto_trans($1_t, hc_diag_sys_exec_t, $1_diag_t)

  domain_entry_file($1_diag_t, hc_diag_sys_exec_t)

  allow $1_diag_t $1_t:process sigchld;

  allow $1_diag_t $1_tty_device_t:chr_file { rw_term_perms append };

  allow $1_diag_t $1_devpts_t:chr_file { rw_term_perms append };

}
```

6.5 Analysis

To meet real-world application security demands that are understandable, implementable and usable, our OTHIS research embraces reasonable security strategies against economic realities using open solution technologies such as SELinux rather than using proprietary technologies. In general, open source technologies are free to use, modify, and redistribute. Developers of open source software distribute their software freely and make profits from support contracts and customised development. It is an expensive exercise to use proprietary software in particular for large enterprises to upgrade software and increase its number of software licenses. The costs of using proprietary software involve the procurement of a software license and software upgrades. Open source technologies have gained significant attention in the marketplace. A Gartner report[37]predicts that more than 90 percent of enterprises will use open source in direct

[37] A ZDNet new article “A Gartner: Open source will quietly take over” is available at http://news.zdnet.co.uk/software/0,1000000121,39379900,00.htm accessed 29/08/2008.

embedded ways by 2012. In particular, open source software is essential for large enterprises who seek to reduce their total cost of ownership and increase returns on investment. A common complaint related to open source is the lack of a reliable source of assistance when organisations encounter problems in open source software. One can resolve this through the subscription of service support from the open source developer.

It is essential to integrate security profiling structures in relation to other enterprise systems such as overall human resource management systems and the like. This allows for definition and deployment of security policies that represent legal, regulatory, policy and enterprise level requirements for reliable and consistent enforcement at the computer system level. The primary and well-known strength of SELinux is security, yet the level of complexity in policy configuration could be considered beyond the expertise level of many CIOs in health related organisations. Simplifying the level of complexity in SELinux configuration can be managed through the current distribution containing the SELinux Reference Policy. This is an example of a general purpose security policy configuration which can meet a number of security objectives and can be used as the basis for creating other policies. Additionally, there is a number of SELinux Policy generation and management tools[38] available to simplify the development of SELinux Policy.

Currently, the Flask architecture with the Flexible MAC enforcement is a rapidly growing area gaining global attention since its introduction in SELinux. A recent press release[39] issued in 2008 announced that Flask will also be implemented in Sun Microsystems OpenSolar operating system to advance MAC. Thus, tools and techniques are constantly developed from the open source community to address the complex configuration challenges of SELinux. In fact, our HIAC proof-of-concept prototype for HIS was built on RHEL version 4, which was carried out at the primitive stage of SELinux project development [9]. It was argued that the previous SELinux policy

[38] Links to SELinux Policy generation tools are available at http://fedoraproject.org/wiki/SELinux/PolicyGenTools accessed 27/08/2008.

[39] A media release has been issue announcing the joint venture between the NSA and Sun Microsystems to advance MAC named “National Security Agency And Sun Microsystems Lead OpenSolaris Community Project To Advance Mandatory Access Controls” is available at http://www.sun.com/aboutsun/pr/2008-03/sunflash.20080313.1.xml accessed 27/08/2008.

facilities were too inflexible to handle a large scale of HIS which may involve dynamic and frequent changes to the security policies such as adding/deleting users and applications. With the earlier SELinux distribution, any changes and extensions made to the SELinux Policy would have needed the policy to be recompiled and the system to be restarted. As SELinux continues to advance and evolve, any changes to the security policies can be recompiled with available tools and techniques and then updated security policies reloaded into the system kernel without the need to restart the system. To date our HIAC proof-of-concept prototype has been updated with Fedora Core 9 to confirm the flexibility of the current release of SELinux.

6.6 Conclusion and Future Work

Current trends are towards using Web Services as the technology to develop and implement healthcare application systems. Their focus is on security aspects in exchanging clinical information electronically at the application level. This is endorsed by NEHTA (2005). The moves towards Service Oriented Architecture/Web Services global systems present major challenges where such structures are not based on highly trusted operating systems. All applications and supporting software which necessarily reside atop the untrusted operating systems are also considered untrusted. Health information is highly sensitive by its nature. It is therefore critical to protect such information from security hazards and privacy threats.

The authors argue that using the non-MAC-based system to protect personal privacy and confidentiality of electronic health records is not sustainable. This is evidenced by a number of scenarios related to health information privacy violations or weaknesses which have recently been found in Australia, the UK and the USA [12]. Our OTHIS/HIAC research argues that the need of a radical re-think is absolutely crucial in the understanding of access control in light of modern information system structures, legislative and regulatory requirements and security operational demands in HIS. This

is affirmed by the Australian Government[40] calls for robust legislation to protect individual electronic health record systems. This security focus enhances the quality of healthcare service delivery with respect to privacy assurance and is a key element of the overall success of such a system.

Information and communications technologies are now sufficiently advanced that a MAC-based electronic healthcare management system is feasible. Our approach overcomes many of the security issues which have plagued previous attempts at electronic health management systems. The authors argue that adoption of appropriate security technologies, including in particular Flexible MAC-oriented operating system bases, can satisfy the requirements for the protection of sensitive health data.

Preliminary results of this research indicate that the broad philosophy of Flexible MAC appears ideally suited to the protection of the healthcare information systems environment. This study, therefore, contends that the approach to "hardening" electronic HIS is essential to build privacy- and security-aware applications that reside atop Flexible MAC-based operating systems. Such systems have the potential to meet all stakeholder requirements including modern information structures, organisational security policies, legislative and regulatory requirements for both healthcare providers' and healthcare consumers' expectations and demands in HIS.

To provide sustainable and trusted health information systems, one must take an holistic approach to address security requirements at all levels in HIS. The overall HIS architecture must evolve into a set of complementary security architectures which, at least, incorporates those proposed under the OTHIS scheme consisting of HIAC, HIAS and HINS. This paper focuses on OTHIS/HIAC which proposes a viable solution to provide appropriate levels of secure access control for the protection of sensitive health data. Future research under OTHIS will continue to develop and test through experimental structures created on a Flexible MAC-based operating system. Key research questions to be answered include those issues of data "at rest"

[40] A press release has been issued entitled "E-health privacy blueprint - robust legislation is needed says Privacy Commissioner" is available at http://www.privacy.gov.au/news/media/2008_15.html accessed 27/08/2008

and “under processing” aspects of the proposed architecture OTHIS. This research will also elucidate the relationships between HIAS which relies completely upon trust in HIAC and HINS.

6.7 References

[1] Steptoe & Johnson LLP, E-Commerce Law Week, Issue 321, 2008. http://www.steptoe.com/publications-3133.html (accessed 2/09/2008).

[2] E. Dyson, Reflections on Privacy 2.0, in Scientific American. 2008. p. 55-60.

[3] NEHTA, Towards an Interoperability Framework. 2005, National E-health Transition Authority.

[4] P. Loscocco, S. Smalley, P.A. Muckelbauer, R.C. Taylor, S.J. Turner, J.F. Farrell, The Inevitability of Failure: the Flawed Assumption of Security in Modern Computing Environments, appeared in: Proceedings of the 21st National Information Systems Security Conference(1998)

[5] D. Goldstein, P. Groen, S. Ponkshe, M. Wine, eds. Medical Informatics 20/20: Quality and Electronic Health Records through Collaboration, Open Solutions, and Innovation. 2007, Jones and Battlett Publishers, Inc.

[6] D. Sharanahan, P. Karvelas, Welfare workers axed for spying, in The Australian. 2006.

[7] D. Leigh, R. Evans, Warning over privacy of 50m patient files, in Guardian News and Media Limited. 2006.

[8] GAO, Information Security: Department of Health and Human Services Needs to Fully Implement Its Program, 2006. http://www.gao.gov/new.items/d06267.pdf (accessed 12/05/2008).

[9] M. Henricksen, W. Caelli, P. Croll, Securing Grid Data Using Mandatory Access Controls, appeared in: 5th Australian Symposium on Grid Computing and e-Research (AusGrid). Ballarat Australia, (2007)

[10] L. Martin Franco, SELinux Policy Management Framework for HIS (under examination) in Faculty of Information Technology. 2008, Queensland University of Technology: Brisbane, Australian.

[11] P. Loscocco, S. Smalley, Meeting Critical Security Objectives with Security-Enhanced Linux, appeared in: Proceedings of the 2001 Ottawa Linux Symposium(2001)

[12] V. Liu, W. Caelli, L. May, P. Croll, A Sustainable Approach to Security and Privacy in Health Information Systems, appeared in: 18th Australasian Conference on Information Systems (ACIS) Toowoomba, Australia, (2007)

Statement of Contribution of Co-Authors for Thesis by Published Paper

In the case of this chapter:

Publication title: A Secure Architecture for Australia's Index Based E-health Environment

Publication status: This conference paper appeared at the Australasian Workshop on Health Informatics and Knowledge Management (HIKM) January 2010, Brisbane Australia.

The authors listed below have certified that:

1. They meet the criteria for authorship in that they have participated in the conception, execution, or interpretation, of at least that part of the publication in their field of expertise;
2. They take public responsibility for their part of the publication, except for the responsible author who accepts overall responsibility for the publication;
3. There are no other authors of the publication according to these criteria;
4. There is no conflicts of interest have been disclosed to (a) granting bodies, (b) the editor or publisher of journals or other publications, and (c) the head of the responsible academic unit, and
5. They agree to the use of the publication in the student's thesis and its publication on the Australasian Digital Thesis database consistent with any limitations set by publisher requirements.

Each author's contributions are listed below:

Contributor	Statement of contribution
Vicky Liu	participated in the conception and design of this manuscript, acquisition of data, analysis and interpretation of the data, writing of this manuscript and acting as the corresponding author
William Caelli	contributed to the conception and design of this manuscript, revising it critically for important intellectual content and final approval of the version to be published
Jason Smith	contributed to the conception and design of this manuscript and revising it critically for important intellectual content
Lauren May	contributed to revising the manuscript critically for important intellectual content
Min Hui Lee	performed data acquisition on literature review information
Zi Hao Ng	performed data acquisition on identifying necessary interoperability requirements for e-health messaging provisioning
Jin Hong Foo	performed data acquisition on literature review information
Weihao Li	performed data acquisition on literature review information

Principal Supervisor Confirmation

I have sighted email or other correspondence from all co-authors confirming their certifying authorship.

W CAELLI		12-8-2010
Name	Signature	Date

Chapter 7 A Secure Architecture for Australia's Index Based E-health Environment

Vicky Liu, William Caelli, Jason Smith, Lauren May, Min Hui Lee, Zi Hao Ng, Jin Hong Foo and Weihao Li

Faculty of Information Technology and Information Security Institute

Queensland University of Technology, Australia

PO Box 2434, Brisbane 4001, Queensland Australia

v.liu@qut.edu.au

Abstract

This paper proposes a security architecture for the basic cross indexing systems emerging as foundational structures in current health information systems. In these systems unique identifiers are issued to healthcare providers and consumers. In most cases, such numbering schemes are national in scope and must therefore necessarily be used via an indexing system to identify records contained in pre-existing local, regional or national health information systems. Most large scale electronic health record systems envisage that such correlation between national healthcare identifiers and pre-existing identifiers will be performed by some centrally administered cross referencing, or index system. This paper is concerned with the security architecture for such indexing servers and the manner in which they interface with pre-existing health systems (including both workstations and servers). The paper proposes two required structures to achieve the goal of a national scale, and secure exchange of electronic health information, including: (a) the employment of high trust computer systems to perform an indexing function, and (b) the development and deployment of an appropriate high trust interface module, a Healthcare Interface Processor (HIP), to be integrated into the connected workstations or servers of healthcare service providers. This proposed architecture is specifically oriented toward requirements identified in the Connectivity

Architecture for Australia's e-health scheme as outlined by NEHTA and the national e-health strategy released by the Australian Health Ministers.

Keywords: architecture of health information systems, security for health information systems, health informatics, network security for health systems, trusted system, indexing based system for e-health regime, HL7

7.1 Introduction

Undoubtedly, the adoption of e-health has much potential to improve healthcare delivery and performance [1, 2]. Anticipated improvements relate to better management and coordination of healthcare information and increased quality and safety of healthcare delivery. On the other hand, a security violation in healthcare records, such as an unauthorised disclosure or unauthorised alteration of individual health information, can significantly undermine both healthcare providers' and consumers' confidence and trust in the e-health system. A crisis in confidence in national e-health systems would seriously degrade the realisation of potential benefits.

Evidence from the NEHTA's Report on Feedback Individual Electronic Health Record [3] suggests that numerous healthcare consumers and providers embrace the adoption of national individual electronic health records because of the potential benefits. There are a number of consumers, however, who are reluctant to embrace e-health because of privacy concerns. Obviously, the security and privacy protection of information is critical to the successful implementation of any e-health initiative. NEHTA, therefore, rightly places security and privacy protection at the centre of its e-health approach.

In order to address the requirements for enabling a secure national e-health environment, we propose a security architecture based around the current strategic directions from the Australian Government's National E-Health Strategy [1] and Connectivity Architecture [4] proposed by NEHTA, both recently released in December 2008.

This proposed architecture defines a model to support secure communications between healthcare providers and the Index System in the national e-health environment, which some other approaches fail to address. We draw on important lessons from the Internet's Domain Name System (DNS) for the development and deployment of the national healthcare Index System. Our approach embraces the hierarchical and distributed nature of DNS and defines the required components for a secure architecture for Australia's national e-health scheme. This proposed architecture employs a high trust computer platform to perform indexing functions and a high trust interface module as the application proxy to connect to the healthcare Index System and other healthcare service providers.

7.2 Paper Structure

This paper begins with a summary of the benefits associated with increased adoption of e-health; however, risks to privacy in such e-health systems must be addressed. Addressing the security appropriately is considered as key to success of the e-health implementation. Section 7.3 defines the paper's scope and details our assumptions in the context of the Australian national e-health environment. Section 7.4 investigates three representative e-health initiatives resembling the approach being adopted in Australia. Section 7.5 reasons the lesson we can learn from Internet's DNS to design the national e-health Index System. The authors' proposal for a secure connectivity architecture with the required structures is described in Section 7.6. Section 7.7 illustrates a request for a specific patient's health records via the Index System with a set of information flows. The analysis of this work is incorporated in Section 7.8. Finally, the conclusion is drawn and future direction for work is outlined in Section 7.9.

7.3 Scope and Assumptions

The Australian National E-heath Strategy [1] defines the basic building blocks for a national e-health system including: (1) the implementation of the healthcare identifier (HI) scheme for healthcare consumers and providers, (2) the establishment of standards for the consistent collection and exchange of health information, (3) the establishment of rules and protocols for secure

healthcare information exchange, and (4) the implementation of underlying physical computing and network infrastructure. We propose a secure architecture to address the protection of clinical information exchange in a reliable and secure manner. This proposed architecture is specifically concerned with the secure architecture design and development to facilitate interactions between healthcare providers, healthcare organisations and the national Index System rather than focusing on healthcare consumers accessing healthcare information.

It is anticipated that the national HI scheme will be established by mid 2010 [5]. This paper assumes that an adequate national legislative framework will be established to support the management and operation of the healthcare identifier scheme [6] to enable a national e-health implementation by July 2010. Presumably, the National Authentication Service for Health (NASH) becomes available for Public Key Infrastructure (PKI) services to support digital signing and data encryption in the national e-health environment. It is also assumed that the National Broadband Network (NBN) infrastructure will be constructed for electronically enabling access and transfer of health information nationally.

In the context of this paper, a service requester refers to the entity that uses a service provided by another entity. A service provider is an entity that offers a service used by another entity. A service provider can be a healthcare provider, healthcare organisation or organisation commissioned to provide services for healthcare providers or healthcare organisations.

7.4 Related Work

While most nations would appear to have some e-health initiatives at some stage of investigation or implementation, this section focuses on three national e-health architectures resembling the approach being adopted in Australia.

7.4.1 Dutch National E-health Strategy

The Dutch e-health infrastructure is constructed by the National IT Institute for Healthcare in the Netherlands (NICTIZ)[42]. The Dutch national e-health approach uses the National Healthcare Information Hub, National Switch Point (Landelijk SchakelPunt or LSP) to enable the exchange of healthcare information. There is no clinical information stored at the LSP. The clinical data details reside at local health information systems. The Dutch national index system, LSP, includes services such as identification and authentication, authorisation, addressing, logging and standardization of messages services [7]

The LSP links healthcare providers' information systems together to enable the electronic exchange of health information nationally. The Dutch national e-health network connectivity architecture requires the healthcare partitioners' health information system to comply with the security requirements for a "Qualified Health Information System to be allowed to connect to the LSP via a qualified commercial service provider. Such IT service providers are commissioned to provide secure communications between healthcare information systems and the LSP" [8] .

While the healthcare provider requests specific patient information which is located in other healthcare information systems, all queries are relayed via the LSP. The healthcare service provider responds to the LSP. Namely, the LSP aggregates the requested health data from the health service providers and then routes the health data to the requester. There is no direct communication between the healthcare service providing system and requesting system. The LSP also logs which healthcare practitioners have accessed patient data for accountability [9].

The Dutch national index system, LSP, is the central coordination point for exchange health information, including authentication, authorisation, routing and logging. Such an implementation model may appear suitable for a small

[42] NICTIZ is Dutch national e-health coordination point and knowledge centre. The related information is available at http://www.nictiz.nl/, accessed 28/08/2009.

scale of national e-health structure. Implementation of this model in a geographically large country will produce more network traffic, possibly creating performance bottlenecks; it is particularly prone to a single point of failure weakness.

7.4.2 National Health Service (NHS) in England

The National Health Service (NHS) in England implements the National Programme for IT (NPfIT) to deliver the central electronic healthcare record system. This central system is known as Spine. Spine provides national e-health services in England including:

- The Personal Demographics Service (PDS), which stores patients' demographic information including unique patient identifiers - NHS Numbers;
- Spine Directory Services (SDS), which provides directory services for registered healthcare providers and organisations;
- National Care Record (NCR), which contains clinical information summaries as well as the location of the detailed healthcare information;
- Legitimate Relationship Service (LRS), which is an authorisation logic containing details of relationships between healthcare professionals and patients and patient preferences on information accessing; and
- Transaction and Messaging Spine (TMS), which provides routing for querying and responding to clinical messages via the NCR [10].

The English national e-health services include identification and authentication, authorisation logic, clinical summary information, directory services and routing. This programme is implemented in England, while Wales is running another national programme. The separate provisions of national e-health systems need to be made interoperable for information traversing across national borders.

7.4.3 USA Health Information Exchange (HIE)

USA National Institute for Standards and Technology (NIST) recently released a document entitled Draft Security Architecture Design Process for Health Information Exchanges (HIEs) [11] to provide guidance for the development of a security architecture particularly for the exchange of healthcare information. The HIE security architecture design process includes five layers to construct a security architecture for healthcare information exchange. The five layers include: (a) policies for overall legal requirements to protect healthcare information access, (b) services and mechanisms to meet policy requirements, (c) operational specifications for the business processes, (d) definitions of technical constructs and relationships to implement enabling processes, and (e) provisions for technical solutions and data standards for implementing the architecture.

USA health information exchange architecture is based upon a hierarchical structure. Namely, it consists of a National Federation Health Information Exchange (HIE), Multi-Regional Federation HIEs, and Regional HIEs. The National Federation HIE, national federated technical architecture, connects a number of Multi-Regional Federation HIEs, involving multiple states jurisdictions. Multi-Regional Federation HIEs connect multiple regional HIEs. Regional HIEs can consist of two or more independent healthcare providers to share healthcare information. The participating healthcare providers set up their own trust agreement to define security and privacy requirements for the exchange of healthcare information [11] .

The Identity Federation Service provides identification and authentication services. The entity can be authenticated via the Identity Federation Service or its home organisation's authentication service to support single sign on for accessing the HIE services. The privilege management is performed by service providers locally [11].

The USA approach is different from the Dutch and English national e-health architectures. In a large nation like the USA, the distributed national e-health scheme seems suitable for scalability. USA e-health architecture is similar to

the context of the DNS hierarchical model. This type of approach can mitigate the network traffic and performance bottleneck on the centralised e-health system.

7.5 Lesson Learnt from the Internet's Domain Name System (DNS)

The Internet's *"Domain Name System (DNS)"* has become a critical part of the Internet and of the *"World Wide Web (WWW)"* in particular. Without its services many current information systems and services provided over the Internet would not function. Indeed, as Web-based applications rapidly become the "norm", particularly in the public sector but also in the private sector, the resilience and high speed performance of the DNS have become mandatory requirements. The use of Web-based structures has been nominated as the basic functional structure of the Australia Federal e-health, NEHTA scheme. The DNS structure, determined some 25 years ago, is based around a globally distributed, hierarchical database architecture that relies upon replication for resilience and caching for performance. However, it has been realised that the basic DNS scheme is insecure, in the sense that both confidentiality and integrity, including authenticity and authorisation, were not part of the overall design during the original design and development time of the early to mid 1980s.

"Robustness and adequate performance are achieved through replication and caching" [12]. Essentially, the client-server model chosen, via use of client "resolvers" and then "name-servers", has been proven over time and is the model suggested in this architecture. The hierarchical nature of the DNS structure again appears suitable given that the Australian system must cater for a federated national structure with roles for the various State level participants. The *"ccTLD"* or *"country top level domain"* coupled with a "2nd level" structure appears to offer suitable benefits in organisation and management as well as the necessary backup resilience that is required in the overall scheme.

The appropriate security arrangements, the *"Transaction Signatures (TSIG)"* structure based on a single-key cryptographic system again helps in this

regard in relation to the secure synchronisation of actual DNS nameserver systems themselves. As Liu and Albitz (2006) state, *"TSIG uses shared secrets and a one-way hash function to authenticate DNS messages, particularly responses and updates."* Similar schemes exist for confidentiality, integrity and authenticity services in data networks in the banking and finance sector.

As mentioned above, the original DNS structure did not consider matters of confidentiality and integrity. At the same time, the TSIG scheme is not scalable to any real dimension as nameservers correspond with an arbitrary set of other nameservers. The *"DNS Security Extensions (DNSSEC)* [13-15]*"*, through use of "Public Key Cryptography", enable DNS "zones" to "digitally sign" the necessary nameserver tables so that, on distribution, such tables can be checked for authenticity and integrity by the receiver. The addition of appropriate DNSSEC records to the overall database structure provides a useful model that may be incorporated into the proposed architecture that is the subject of this paper.

In summary, the overall DNS experience, and the structure of the DNSSEC security extensions provide a most suitable model for incorporation, in modified form, into the healthcare index architecture proposed. The DNSSEC structure assists in combating known attacks on the Internet system through such techniques as "cache poisoning", "traffic diversion", "man-in-the-middle attacks" and so on. At the same time, however, the basic index systems, like the Internet's DNS nameserver systems, must be installed and managed on basic computer systems, including the necessary operating systems (OS) that are sufficiently secure for the purpose. The immediate use of DNSSEC style structures is seen as essential given that many aspects of the proposed e-health record infrastructure will reside on the general purpose Internet.

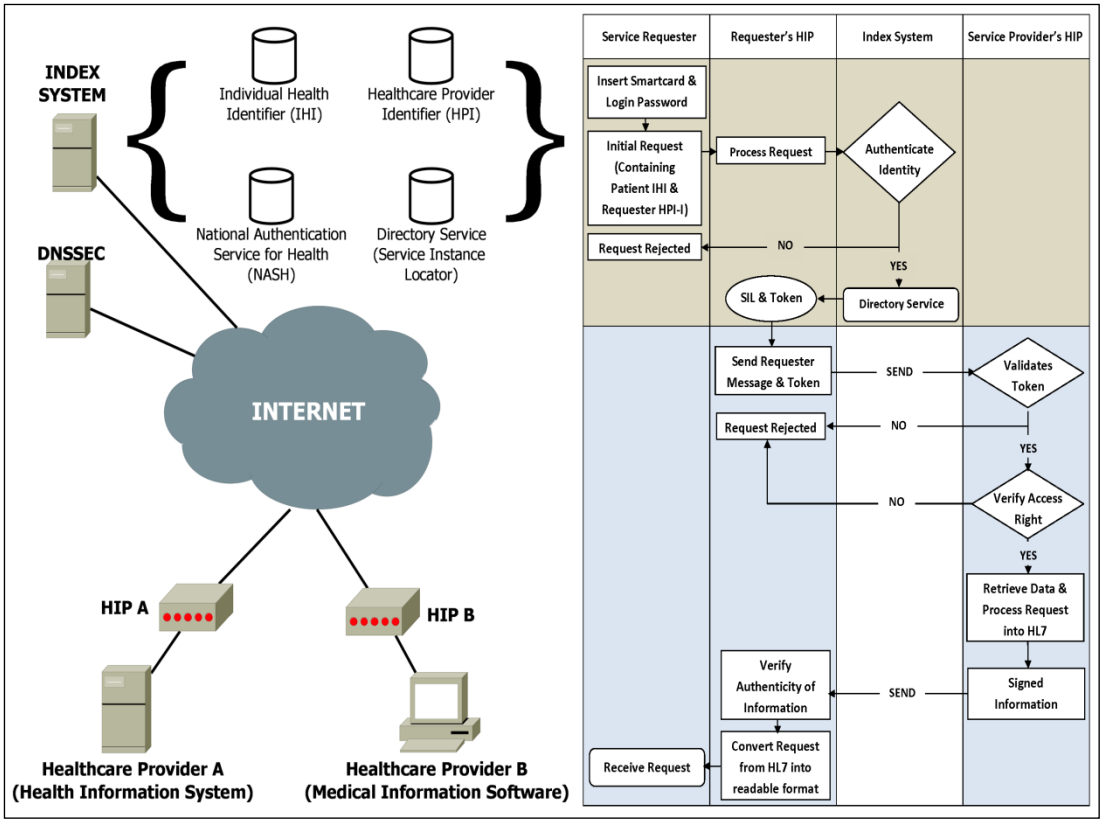


Figure 11: Proposed Architecture Overview and Key Information Flows

7.6 Our Approach

Generally, health information is stored over a number of different health information systems. A national index system must be available for the provision of directory services to determine the distributed locations of the source systems holding the related health records. Our proposal addresses this need by defining a model to support secure communications between healthcare providers and the Index System in the national e-health environment as shown in Figure 11. This proposed architecture is based on the broad architecture of the Australian Government's National E-health Strategy [1] and NEHTA's Connectivity Architecture[4], both released in December 2008.

Our proposed architecture defines the required constructs to share and transfer healthcare information securely between healthcare providers and the authorised national Index System. This architecture proposes that the Index System should be built on a high trust computer platform as well as mandating that the participating healthcare providers need to adopt a high

trust interface module - HIP as the application proxy to link to the Index System and other health information systems. Additionally, the authors argue that a fundamental security issue, that of name resolution, must be addressed prior to the interactions between the healthcare providers and national Index System. This paper, therefore, proposes a trusted architecture not only providing the indexing service but also incorporating a trusted name resolution scheme for the enforcement of communicating to the authorised Index System.

Since the Index System is itself a critical application under any operating system, that Index System must be protected from even internal threats through the use of modern “flexible mandatory access control (FMAC)” structures. Under such an operating system, and as distinct from the less secure “discretionary access control (DAC)” systems, even a systems manager may not have permission to access the health record data. In simple terms, in these systems there is no “super-user” capable of obtaining access to all system resources at any time. If an individual nameserver system is “captured”, propagation of exposure will not extend beyond the compromised application itself, a vital concern in any e-health record indexing structure. Such systems exist and are commercially available, e.g. the “Secure LINUX (SELinux)” systems, “Solaris/SE” system, etc. The proposed “HIP” structure would make use of such security enforcement to provide the necessary protection levels.

7.6.1 Index System (IS)

The authors argue that the load of the national Index System should be relatively lightweight to perform e-health indexing services efficiently. This can mitigate the Index System explosion and traffic bottleneck risks. Such an approach is favourable in a geographically large country such as Australia. To maximise the efficiency of the indexing services, the proposed Index System does not provide network connectivity services, messaging translation, addressing and routing functions and extensive logging of all message access. These services can be performed at the level of the local health information systems via the HIP, which is detailed in Section 7.2. The

access control and authorisation process is best performed close to where the source system is, as each healthcare service provider might implement the service differently based on its own health information system access requirements. NEHTA [4] also states that there are no centralized network provisions to handle peer-to-peer communications; each service must manage its own interface to the network.

The Index System will be a centralised facility run at a national level. It is envisioned that the directory service is devised in the context of a DNS, which uses hierarchical distributed database architecture.

Our proposed national Index System performs common and fundamental functionalities including:

- Identification and authentication, and
- Directory services.

7.6.1.1 Identification and Authentication Services

The national Healthcare Identifiers Service (HI Service) is indeed one of the building blocks for the national e-health infrastructure. The national HI scheme for identification services must be deployed prior to the implementation of the national e-health system. The HI Service will provide accurate identification of individuals and healthcare providers in the national e-health environment.

Individuals receiving healthcare services will be assigned an Individual Healthcare Identifier (IHI). All authorised Healthcare providers will receive a Healthcare Provider Identifier – Individual (HPI-I). Healthcare centres and organisations in Australia will be provided with a Healthcare Provider Identifier – Organisation (HPI-O). To be eligible to query the HI Service, a requesting entity must be nominated by a healthcare organisation and have an HPI-I associated with an HPI-O. The IHI Service will allow authenticated healthcare providers to lookup a specific IHI. The HPI Service of the Index System will provide lookup services to navigate the locations of healthcare

providers to facilitate communication and the exchange of healthcare information [16].

National Authentication Service for Health (NASH) is designed by NEHTA to provide PKI authentication services. NASH will issue digital certificates and tokens for registered and certified healthcare providers and organisations [16].

7.6.1.2 Directory Services

The Directory Service is one of the fundamental services in national e-health infrastructure. Since healthcare data are located at various places, directory services are used to identify and locate the available information. The Directory Service in the Index System provides a mechanism for obtaining the necessary information for invoking a service. This information contains the network location of the service, the digital certificate required to use it and other information required to invoke the service. It is envisaged this will be specified in Web Services Description Language[43] (WSDL) format, which equates to Service Instance Locator (SIL) [17] functionalities outlined by NETHA.

7.6.1.3 Operation of the Directory Services

Based upon NEHTA's definitions [18] on concepts and patterns for implementing services, the service patterns can be divided into two broad categories: synchronous and asynchronous services. A synchronous service occurs in direct response to a request. An asynchronous service has no relationship between the events. For example, to request a specific individual's health records is a synchronous service. To send out a discharge summary report to a healthcare provider is an asynchronous service.

With a synchronous service, when interacting with the directory service the requesting entity will provide proof of their identity (HPI-O) and the IHI associated with the records they are requesting. Once the requester has

[43] WDSL is used for describing how to access the network services in XML format. More detail is available at http://www.w3.org/TR/wsdl#_introduction accessed 30/08/2009.

been authenticated by the Index Server, it will respond with the following: (a) a signed token attesting to the identity of the requester ({token}$Sign_{IS\_PrivKey}$) and (b) a list of service instances containing health records for the person identified by the IHI (Service_Instance_1,...,Service_Instance_N).

The entire response is signed so that the requester can be assured that it is a legitimate response from an authorised Index System and that any alterations to the response will be detectable. The response is also encrypted under a key known by the requester ({...}$Encrypt_{HPI\text{-}O\_PubKey}$), in order that the confidentiality of both the requester and the individual identified by the IHI is maintained.

The token is signed independently of the entire response in order that it can be reused with requests to each service instance. The full response is depicted in Figure 12.

$$\{\{token\}Sign_{IS\_PrivKey}, Service\_Instance\_1, \ldots, Service\_Instance\_N\}Encrypt_{HPI\text{-}O\_PubKey}$$

Figure 12: Service Instance Response Message Format

The service instance information contained in the response identifies the target system location and information necessary for securely invoking that service. This may include, but will not be limited to the credentials / certificates required to access the service. The signed token provided in the Index System response may be the only credential required, in which case the effort expended by the Index System in authenticating the requester is reused. It is, however, conceivable that additional authentication may be required by a given service instance. For example, the requester may need to prove that they are a member of a given practice or college of medical practitioners.

With an asynchronous service, such as when a discharge summary message needs to be sent to the patient's primary healthcare provider, the healthcare provider issuing the summary queries the Index System for the

primary healthcare provider's HPI, location and the digital certificate and then signs and encrypts the discharge message prior to transmission.

7.6.2 Healthcare Interface Processor (HIP) – Proxy Service

Our design philosophy of HIP draws on principles used in the Interface Message Processor (IMP) of the Advanced Research Projects Agency Network (ARPANET). Each site uses an IMP to connect to the ARPANET network in order to isolate the potential hostile system connecting the ARPANET network. Our design rationale underlying HIP is to provide a secured communication channel for an untrusted health information system connected to the Index System as well as for health information exchange between healthcare providers. Wherever a connection to the national indexing system is required, a HIP facility has to exist. The design goal for HIP is to make it as a "plug and operate" facility, which is easy and simple to use for healthcare providers as well as with characteristics of high security, reliability, efficiency and resilience. Such a design would be very beneficial and useful particularly for healthcare providers.

HIP contains its own on-board crypto-processor based on a trusted computing based module to store cryptographic keys. Any information system depends, therefore, upon a trusted base for safe and reliable operation, commonly referred to as a "trusted computing-base". Without a trusted computing base any system is subject to compromise. For this reason HIP aims to run on top of trusted hardware, firmware and operating system. HIP, a self-contained unit configured with an IP address, is capable of running Web services. HIP carries out its works from layer 1 to 7 of the seven-layer OSI model.

It is envisaged that HIP achieves provisions of security services and mechanisms based upon the security and management concepts of the OSI IS7498-2, including:

- To establish a **trusted path** to connect to the authorised Index System,

- To provide **peer-entity authentication** between healthcare providers and national Index System,
- To facilitate secure healthcare information exchange in transit,
- To provide **data protection** with appropriate **access control** mechanisms,
- To provide **interoperability** to enable healthcare information exchange between disparate healthcare systems with varying security mechanisms,
- To support **accountability** when healthcare information has been accessed, and
- To provide **operation flexibility** with "emergency override" and **capacity flexibility** for various scales of healthcare organizations.

7.6.2.1 Trusted Path Establishment

In response to the recent increase in DNS cache poisoning and traffic diversion attacks, we propose that the first step is to perform the enforcement of communicating to the authorised Index System prior to the interactions between the service requesting entity and the Index System. To achieve this, from a technical underlying process, HIP should be pre-configured to contact a DNSSEC capable server to perform a trusted name resolution in order to defend against false DNS data and assure that connections are only established with the legitimate Index System.

7.6.2.2 Peer-Entity Authentication

Many proposals are only concerned with the authenticity of the requesting entity (i.e. one-way authentication) but fail to address the importance of two-way authentication. Our proposed architecture provides a mutual peer-entity authentication service complying with the ISO 7489-2. To authenticate the authenticity of the Index System, the service requesting entity must validate the certificate of the Index System. Once the authenticity of the national Index System is assured, the Index System authenticates the identity of the healthcare service requesting entity. In this sense, the authentication service

of the Index System acts as a notarization mechanism in line with the philosophy of peer-entity authentication stated in ISO IS7498-2.

7.6.2.3 Secured Communication Channel for Health Information Exchange

The healthcare provider's computer may have its security compromised. HIP, a hardened and qualified facility, acts as a proxy server establishing a secured communication channel connecting to the Index System and bringing isolation from the untrusted computer.

HIP will be assigned a standard unique identifier (i.e. HPI-O) and be issued an asymmetric key pair for digitally signing and encrypting to achieve integrity and confidentiality goals. HIP contains its own on-board crypto-processor, thus it can facilitate the secure exchange of health information. In addition, HIP is built on the Trusted Platform Module (TPM) that is used to store cryptographic keys.

7.6.2.4 Provision of Data Protection

As various healthcare organisations may have their own specific access authorisation requirements and processes, access authorisation is best performed where the resource system is located. Once the requesting entity's identity is authenticated, the request of particular healthcare information is presented to the target service provider. The HIP of the target service provider will provide the verified identity and the profile of the requester to the authorisation logic unit to perform access decision making. The authorisation decision depends upon the requesting entity's profile and defined privilege management policy. The implementation of the authorisation logic unit is based on the "Sensitivity Label" function outlined by NEHTA [3].

7.6.2.5 Interoperability Platform

NEHTA[44] is responsible for selecting electronic messaging standards in Australia's health sector. It has endorsed Health Level 7 (HL7) [45] as the national standard for the electronic exchange of health information. HIP provides an interoperability platform by incorporating an HL7 Interface Engine and Message Mapping Sets conforming to the HL7 v3 Message Standards for healthcare information exchange. HIP also incorporates an HL7 Interface Engine and Message Mapping Sets for messaging Interoperability.

HL7 Interface Engine

Any non-HL7-compliant data contents are translated into the HL7 standard format (XML-based data structure) by the HL7 Interface Engine prior to information transmission. The HL7 Interface Engine contains a set of mapping algorithms to map data contents with an appropriate HL7 Message Template to generate an HL7 message.

Message Mapping Sets

The Message Mapping Sets contain a repository of HL7 Message Templates for various clinical and administrative messages. Each set provides one HL7 Message Template to serve for one clinical or administrative message. Message Mapping Sets will be designed and developed to meet the current healthcare service needs and will be imported into HIP. The HL7 Message Template guides and directs data contents to form an HL7 message.

HL7 Clinical Document Architecture (CDA)

HL7 Clinical Document Architecture (CDA) provides a framework for clinical document exchange. HIP imports the HL7 message into a CDA document. This CDA document is also associated with an appropriate stylesheet. The

[44]NEHTA Sets Direction for Electronic Messaging in Health is available at http://www.nehta.gov.au/nehta-news/423-nehta-sets-direction-for-electronic-messaging-in-health, accessed 19/08/2009

[45] Health Level 7, an American National Standards Institute accredited standard, has been developed to enable disparate healthcare applications to exchange key sets of clinical and administrative data.

CDA document and the stylesheet will be sent to the requesting entity through Web services. The requesting entity renders the received document with the stylesheet in a human-readable form with a Web browser.

7.6.2.6 Privacy Accountability

Audit trail mechanisms can be used to deter unauthorised access to data to improve privacy accountability. To enforce privacy accountability, HIP could be configured to automatically trigger an audit trail event particularly when data is being accessed.

7.6.2.7 Operation and Capacity Flexibility

HIP aims to accommodate emergency override whereby any delays that may potentially occur through authentication and authorisation may be overridden. This is particularly relevant in the case of defined emergency including pandemic circumstances. HIP is designed to provide an emergency override provision called “Hit-the-HIP” for ease of operation.

The HIP architecture is flexible enough to cater for interfacing at various levels. Examples of healthcare organisational structures include a one-person general practice clinic, and small or medium clinics to large hospitals. It is proposed that a number of design variations for the HIP facilities, depending on the healthcare structure, may include:

- One-person healthcare practitioner,
- Smaller healthcare practitioners,
- Hospital administration, and
- Regional hospital administration

7.7 Envisioned Key Information Flows

This section uses a scenario to illustrate the key information flows (see Figure 11) based on the proposed architecture described in Section 7.6. While a requester needs to inquire about a specific patient’s health information, the key information flows of the interactions between the requester, Index System and service provider are illustrated in the following

steps. Note that all request and response messages prior to transmission are signed and encrypted for confidentiality, authentication and message integrity reasons.

1. Peer-Entity Authentication Process

    1.1 Prior to peer-entity authentication, to ensure the secure resolution, the service requester's HIP obtains the address of the Index System from the DNSSEC system which is pre-configured in the HIP.

    1.2 The service requester initiates a connection with the Index System via the service requester's HIP. To ensure the authenticity of the Index System, the service requester's HIP validates the certificate of the Index System.

    1.3 To ensure the identity of the service requester, the service requester logs into the Index System with his/her smart card containing their credentials.

2. Health Record Enquiry Process

    2.1 The service request, containing the patient's IHI and requester's HPI-I, is sent to the Directory Services of the Index System to inquire which health providers hold the health records of the specific patient.

    2.2 The Directory Services of the Index System responds with a token and a list of the service instance information for service invocation to the requesting entity. This token indicates the requester identity assertion to enable single sign on for service invocation.

    2.3 The requester verifies the received information and then contacts each target service provider for service invocation. The requester sends the request including the token with other necessary information to invoke the service.

3. Provision of Requested Health Record Process

3.1 Each target service provider validates the request message containing the token and other necessary information for service invocation. In turn, the request is passed to the authorization logic to make an access authorisation decision based on the service requester's profile indicated in the ticket and any additional authorisation attributes which are mutually agreed by the policy.

4. Provision of Requested Health Record Process

4.1 If the access is granted, the service provider extracts the health record from the data source.
4.2 The service provider processes the requested health record into the HL7 message format.
4.3 The target service provider sends the signed and encrypted information to the requester.
4.4 The service provider records the information access for auditing purposes.

5. Provision of Requested Health Record Process

5.1 The requested information arrives at the service requester's HIP.
5.2 The service requester's HIP verifies the information arrived and then extracts the requested information which is in HL7 message format.
5.3 The message must be presented in a human readable format. The representation of HL7 message is rendered and displayed to the requester.

7.8 Analysis

A first point of contact in any Index System must be itself verified for authenticity and integrity. In Internet terms the client system must be sure that it is connected to the correct Index System and not to some fraudulent system or via some intermediate node point capable of monitoring all traffic. The suggestion for use of a DNSSEC style structure in the overall architecture is seen as a minimum requirement for overall trust in the system.

In turn, this implies that all systems used in the creation and operation of a "centralised" Index System must be security verified in line with accepted international standards. The main such standard is the *"Common Criteria (CC)"* set,[46] under international standard IS-15408, accepted by many nations[47] as the base for evaluation of the security stance of any system. Isolation of critical security functions into verifiable hardware and software structures capable of CC *"protection profile"* definition is envisaged along with the acceptance of a requirement for an associated evaluation at a minimum of an evaluation level of "EAL5". This would apply to the HIP. It should also be a requirement that the USA's "FIPS 140-2", the Federal Information Processing Standard, be used for the security verification of cryptographic functions, in line with accepted industry practice.

Unlike previous structures, the HIP may operate at all seven layers of the OSI model and, indeed, be seen as a "proxy" for Internet interaction. For example, the functionalities of HIP include:

- Routing control functions operating at layer 3, the "network layer" of the OSI model;
- HL7 interpreter functions working at the "presentation layer", layer 6;
- Web service operations carried out at layer 7 of the OSI model, the "application layer"; and
- The encryption/decryption mechanisms at layers 2, 3 and 4 of the OSI model.

The proposed structure is cognisant of NEHTA's architectural designs for the overall national health record index scheme proposed for Australia. Moreover, the main aim of the HIP concept is to simplify overall security control and management of the e-health environment from the point of view of those health professionals and practitioners who will be using the system

[46] The Common Criteria Portal is available at – http://www.commoncriteriaportal.org, accessed 7/09/2009.
[47] More information about the Mutual Recognition and the Common Criteria Recognition Arrangement is available at http://www.dsd.gov.au/infosec/evaluation_services/aisep_pages/aisep_partners.html accessed 07/09/2009.

in the future. The whole HIP architecture is seen as being able to be explained and understood by health professionals and related people who are not ICT experts. Moreover, the HIP and its security should be transparent to them in normal operation. The goal of the proposed system is to make the HIP understandable and essentially transparent to users so that health practitioners can focus on their primary functions to deliver quality healthcare service. In this regard, control and management of the overall system is vested in appropriate information and network systems professionals, not the end users or health partitioners themselves.

7.9 Conclusion and Future Work

This paper proposes three distinct suggestions on the architecture set:

(1) Trusted domain name services are a critical element in the overall trusted architecture of any indexing based healthcare systems to combat name resolution cache poisoning and traffic diversion attacks;
(2) A trusted architecture for the Index System which provides the critical solution to determine the locations of distributed health records. This Index System plays a vital role in the national e-health scheme for identification and authentication and directory services. The Index System, therefore, must be a high trust system running on a trusted platform; and
(3) HIP plays a vital role as a proxy server connecting to the national Index System as well as linking to untrusted health information systems. The proposed "HIP" structure will be built on top of a trusted platform. This makes use of available security enforcement to provide the necessary protection levels.

We envisage that the HIP would be subject to security functionalities and evaluation at the minimum requirements of EAL5 under the Common Criteria/ISO15408[48], in which Australia participates under the Common Criteria Recognition Agreement (CCRA)[49].

[48] The international standard ISO15408 sets a strict guideline for evaluating security policy, program design documents, source code, manuals and other factors.
[49] The Common Criteria Recognition Agreement (CCRA) Web site is available at http://www.commoncriteriaportal.org/theccra.html, accessed 03/09/2009.

There are a number of proposals to maintain summarised healthcare records within the overall index system/switching system [8, 10]. A summary of healthcare records in Australia is called an Individual Electronic Health Record (IEHR) [1]. Our architecture can accommodate IEHR: for example an IEHR database added in Figure 11. This proposal needs to be further examined in light of prior experience in other sectors, such as banking and finance industries. While it would appear possible to maintain IEHRs within the national Index System, practicality may indicate that, in line with the DNS system discussed in this paper and in the banking sector, IEHRs may be best implemented at the point where such aggregation is most feasible. In Australia, this would indicate, in light of the DNS system, a second level Index System at the state level which would also contain IEHRs. Under investigation in the overall project is the feasibility of aggregating IEHRs on demand for the use of point access.

Point of Sale (EFTPOS) is a model that can be used to develop HIPs. Part of our future work is to design a prototype to demonstrate this. This paper forms a foundation for the creation of such a prototype/demonstrator high trusted Index System coupled with a prototype HIP. This will form a base of future requests for research funding. HIP will be developed as proof-of-concept which may be used when tendering for supply and installation. It is suggested that the government will issue the development and testing of HIP which involves the production of 5-6 laboratory prototypes and 50-100 production prototypes. Upon the successful bidder testing, this proposal suggests that the government would issue tenders for the production and installation of HIP. This is based upon the successful experience in the financial sector, in particular, the successful structure and deployment of Australian Electronic Funds Transfer at EFTPOS systems over the last 25 years.

Although this paper concentrates on the Australian national e-health environment from a security perspective, our conclusions could be equally applied to any distributed, indexed based healthcare information systems involving cross referencing of disparate health data collections or repositories.

7.10 References

[1] Australian Health Ministers' Advisory Council, National E-Health Strategy Summary, 2008. http://www.health.gov.au/internet/main/publishing.nsf/Content/National+Ehealth+Strategy (accessed 1/09/2009).

[2] D. Goldstein, P. Groen, S. Ponkshe, M. Wine, eds. Medical Informatics 20/20: Quality and Electronic Health Records through Collaboration, Open Solutions, and Innovation. 2007, Jones and Battlett Publishers, Inc.

[3] NEHTA, Report on Feedback Individual Electronic Health Record. 2008, issued by the National Health and Hospitals Reform Commission

[4] National E-health Transition Authority, Connectivity Architecture Version 1.0 - 1 December 2008 Release, 2008. http://www.nehta.gov.au/component/.../624-connectivity-architecture-v10- (accessed 18/08/2008).

[5] Australian Health Ministers' Advisory Council, Healthcare Identifiers and Privacy: Discussion paper on Proposals for Legislative Support, 2009. http://www.health.gov.au/internet/main/publishing.nsf/Content/pacd-ehealth-consultation/$File/Typeset%20discussion%20paper%20-%20public%20release%20version%20070709.pdf (accessed 10/10/2010).

[6] NHHRC, A Healthier Future for All Australians – Final Report 2009. http://www.nhhrc.org.au/internet/nhhrc/publishing.nsf/Content/nhhrc-report (accessed 13/08/2009).

[7] The Dutch Ministry of Health, Overview of the Architecture on Dutch National E-health, 2007 (accessed 25/08/2009).

[8] R. Spronk, AORTA, the Dutch national infrastructure, 2008. http://www.ringholm.de/docs/00980_en.htm (accessed 20/08/2009).

[9] Dutch Ministry of Health, Overview of the Architecture on Dutch National E-health, 2007. http://www.uziregister.nl/Images/emd_wdh_uk_tcm38-17362.wmv (accessed 25/08/2009).

[10] R. Spronk, The Spine, an English National Programme, 2007. http://www.ringholm.de/docs/00970_en.htm (accessed 30/08/2009).

[11] M. Scholl, K. Stine, K. Lin, D. Steinberg, Draft Security Architecture Design Process for Health Information Exchanges (HIEs), 2009. http://csrc.nist.gov/publications/drafts/nistir-7497/Draft-NISTIR-7497.pdf (accessed 5/09/2009).

[12] C. Liu, P. Albitz, DNS and BIND. 2006: O'Reilly Media Inc.,.

[13] R. Arends, R. Austein, M. Larson, D. Massey, S. Rose, RFC4033 DNS Security Introduction and Requirements, 2005. http://www.ietf.org/rfc/rfc4033.txt (accessed 07/09/2009).

[14] R. Arends, R. Austein, M. Larson, D. Massey, S. Rose, RFC4034 Resource Records for the DNS Security Extensions, 2005. http://www.ietf.org/rfc/rfc4034.txt (accessed 07/09/2009).

[15] R. Arends, R. Austein, M. Larson, D. Massey, S. Rose, RFC4035 Protocol Modifications for the DNS Security Extensions, 2005. http://www.ietf.org/rfc/rfc4035.txt (accessed 07/09/2009).

[16] AHM, Healthcare Identifiers and Privacy: Discussion paper on Proposals for Legislative Support, 2009. www.health.gov.au/.../Typeset%20discussion%20paper%20-%20public%20release%20version%20070709.pdf (accessed 13/08/2009).

[17] NEHTA, Service Instance Locator: Requirements, 2008. www.nehta.gov.au/.../606-service-instance-locator-requirements-v11 (accessed 01/09/2009).

[18] NEHTA, Concepts and Patterns for Implementing Services Version 2.0 draft - 1 September 2008 Draft for Comment, 2008. http://www.nehta.gov.au/component/docman/doc_download/547-service-instance-locator-requirements-v10-draft-archived (accessed 09/09/2009).

Statement of Contribution of Co-Authors for Thesis by Published Paper

In the case of this chapter:

Publication title: A Test Vehicle for Compliance with Resilience Requirements in Index-Based E-health Systems

Publication status: This manuscript is to appear at the 15th Pacific Asia Conference on Information systems (PACIS) in 7-11 July 2011 Brisbane Australia.

The authors listed below have certified that:

1. They meet the criteria for authorship in that they have participated in the conception, execution, or interpretation, of at least that part of the publication in their field of expertise;
2. They take public responsibility for their part of the publication, except for the responsible author who accepts overall responsibility for the publication;
3. There are no other authors of the publication according to these criteria;
4. There is no conflicts of interest have been disclosed to (a) granting bodies, (b) the editor or publisher of journals or other publications, and (c) the head of the responsible academic unit, and
5. They agree to the use of the publication in the student's thesis and its publication on the Australasian Digital Thesis database consistent with any limitations set by publisher requirements.

Each author's contributions are listed below:

Contributor	Statement of contribution
Vicky Liu	participated in the conception and design of this manuscript, acquisition of data, analysis and interpretation of the data, writing of this manuscript and acting as corresponding author
William Caelli	contributed to the conception and design of this manuscript, revising it critically for important intellectual content and final approval of the version to be published
Yingsen Yang	performed data acquisition on the test vehicle development for the proposed security architecture
Lauren May	contributed to revising the manuscript critically for important intellectual content

Principal Supervisor Confirmation

I have sighted email or other correspondence from all co-authors confirming their certifying authorship.

W. CAELLI
Name

Signature

12-8-2010
Date

Chapter 8 A Test Vehicle for Compliance with Resilience Requirements in Index-based E-health Systems

Vicky Liu, William Caelli, Yingsen Yang and, Lauren May
Faculty of Information Technology and Information Security Institute
Queensland University of Technology, Australia
PO Box 2434, Brisbane 4001, Queensland Australia
v.liu@qut.edu.au

Abstract

Increasingly, national and international governments have a strong mandate to develop national e-health systems to enable delivery of much-needed healthcare services. Research is, therefore, needed into appropriate security and reliance structures for the development of health information systems which must be compliant with governmental and alike obligations. The protection of e-health information security is critical to the successful implementation of any e-health initiative. To address this, this paper proposes a security architecture for index-based e-health environments, according to the broad outline of Australia's National E-health Strategy and National E-health Transition Authority (NEHTA)'s Connectivity Architecture. This proposal, however, could be equally applied to any distributed, index-based health information system involving referencing to disparate health information systems. The practicality of the proposed security architecture is supported through an experimental demonstration. This successful prototype completion demonstrates the comprehensibility of the proposed architecture, and the clarity and feasibility of system specifications, in enabling ready development of such a system. This test vehicle has also indicated a number of parameters that need to be considered in any national indexed-based e-health system design with reasonable levels of system security. This paper has identified the need for evaluation of the levels of education, training, and expertise required to create such a system.

Keywords: indexed-based e-health systems, security architecture for health information systems, test vehicle

8.1 Introduction

Numerous countries across the globe have national e-health initiatives at some stage of investigation or implementation. Nations such as Australia, New Zealand, the United Kingdom, the Netherlands, Canada, the United States, and Singapore are active in e-health initiatives. Normally, a national e-health system relies on indexing services to determine the locations of a patient's health records. Indexing services therefore play a central role in enabling disparate health records to become accessible across multiple repositories. Australia's National E-health Strategy [1] also acknowledges that a central indexing or addressing mechanism is needed to link related health records which may reside in one or more locations. Moreover, the security, control and management of these indexing systems are subject to emerging and strict governance imperatives. This paper outlines three national index-based e-health initiatives from Australia, Canada, and Germany, and compares to the authors' approach.

In order to address the requirements for enhanced security in national e-health systems, a security architecture for index-based e-health environments is proposed. This architecture is based on the broad outline of the Australian Government's National E-health Strategy [1] and National E-health Transition Authority (NEHTA)'s Connectivity Architecture [2].[50] This proposal, however, could be equally applied to any distributed, index-based health information system involving referencing to other and disparate health information systems.

This paper assesses the feasibility and comprehensibility of the proposed architecture through the implementation of a small test vehicle. The practicality of the proposed security architecture is demonstrated through the implementation of this test vehicle. This research elucidates a logic process

[50] NEHTA was established to accelerate the adoption and progression of e-health in Australia in 2005.

model with functional specifications to be used as development guidelines and functional assessment for conforming implementations.

Section 8.2 reviews three national index-based e-health initiatives and identifies the relationship of their strategies to the authors' approach. Section 8.3 reports on the test vehicle background which is based on our previous work. The purpose, scope, and selection of software development tool sets of this test vehicle are detailed in Section 8.4. Section 8.5 lists the structure of the test vehicle with logic process modules and provides a description of one exemplary functional requirement specification. Section 8.6 uses two scenarios to illustrate the key information flows within the implementation of the test vehicle. An analysis of the test vehicle implementation is presented in Section 8.7. Finally, our conclusion is presented and suggestions are made for further research.

8.2 Related Work

Numerous countries across the globe have a national e-health initiative at some stage of investigation or implementation. This section outlines three national index-based e-health architectures and identifies the relationship of their strategies to the authors' approach.

8.2.1 Australia's National E-health Strategy

Australia's national e-health approach adopts a concept of a distributed Individual Electronic Health Record (IEHR) which is expected to be developed across geographic regions, according to the strategic directions specified in the Australian Government's National E-Health Strategy [1]. IEHR has been referred to as the Personally-Controlled Electronic Health Record (PCEHR) by the Australian Government [3]. The PCEHR system intends to contain summarised patient health information which aggregates the health records coming from original health information into integrated records across multiple locations. Australia's national e-health strategy also acknowledges that a central indexing or addressing mechanism is needed to link related health records which may reside in one or more locations.

NEHTA provides a design and implementation guide on Endpoint Location Service (ELS) [4] for indexing purposes.

Significantly, the protection of e-health information security plays a critical role in the success of any e-health implementation [5]. In response to this concern, this paper proposes a security architecture for index-based e-health environments, based on the broad outline of Australia's National E-health Strategy [5], NEHTA's Connectivity Architecture [6], and NEHTA's ELS Implementation Guide [4]. The proposed architecture demonstrates a logic model for indexing and supports secure communications between healthcare providers and the Index System (Sections 8.5 and 8.6).

8.2.2 Canadian Electronic Health Record (EHR) Solution

Canada's national e-health architecture, outlined in the Electronic Health Record Solution (EHRS) Blueprint [7, 8], comprises all subsets of jurisdictional EHR systems. Each jurisdictional EHR system consists of integrated and cross-referenced health data replicated from source data systems. Canada's EHRS Blueprint is a highly cross-referencing and index-based scheme linking relevant health records located at various registries and repositories. With Canada's EHR approach, each participating healthcare entity interacts with the jurisdictional EHR system via a message broker called the Health Information Access Layer (HIAL) to upload and retrieve shared health data from the EHR system.

The HIAL element is part of Canada's EHR Infostructure [7, 8], acting as a gateway to provide a collection of services between the EHR services and participating healthcare systems. The technology infrastructure of HIAL exists "in the cloud," and does not reside at the healthcare entity's end. This is in contrast to the proposed Healthcare Interface Processor (HIP) facility. Namely, this research uses a HIP facility which resides at each participating healthcare site to provide a secure communication channel for an untrusted health information system connected to the main Index System. In addition, the proposed HIP facility acts as an interface/gateway for a healthcare

provider's system to connect to other health information systems to exchange health information in a secure and reliable manner.

8.2.3 German National E-health Project

The architecture of the German national e-health project, Telematics [9, 10], comprises three major components:

1. Local health systems connected to the national e-health platform (bIT4Health) for accessing central services of the Telematics infrastructure through a gateway interface, bIT4Health Connector. The Connector, a hardware-based facility or integrated software with an information system, is installed at the local health system site to enable semantic interoperability and to provide data security services;
2. The central Telematics platform provides three subsystems: (i) Generic Common Services; (ii) Common Services; and (iii) Security Services. The Security Services subsystem of interest to this research is needed to access shared health data, such as authentication, authorisation, the signature timestamp, and access logging; and
3. The backend system, which provides a set of resource providers to manage accessible data stores and external services.

The design of the bIT4Health Connector and the proposed HIP facility share the following basic features:

- Both are installed at the local health system site; and
- Both act as a gateway/interface between the central service system and the local health system for the provisioning of semantic interoperability.

In contrast, the major differences between the bIT4Health Connector and the proposed HIP facility are as follows:

- The HIP facility builds on a trusted system to provide a resilient platform to carry out its tasks from Layers 1 to 7 of the seven-layer OSI model; and

- HIP not only intends to enable semantic interoperability for healthcare information exchange, but also provides critical security services, including presenting a trusted path to the national e-health infrastructure, mutual authentication, data protection, accountability, and operational flexibility with an emergency override function.

8.3 Test Vehicle Background

To access an individual's health records from disparate sources, health record indexing services provide lookup services for finding the source locations of health information, and even for the connection requirements for accessing the repository of health data. In our previous paper [11], we proposed a secure architecture for an index based e-health environment based on the strategic directions from the Australian Government's National E-health Strategy [1], and NEHTA's proposed Connectivity Architecture [6] and ELS [4]. Figure 13 illustrates the proposed connectivity architecture with the required structures to support secure communications in the national e-health environment, including: (i) The Index System itself; and (ii) the proposed Healthcare Interface Processor (HIP) facility.

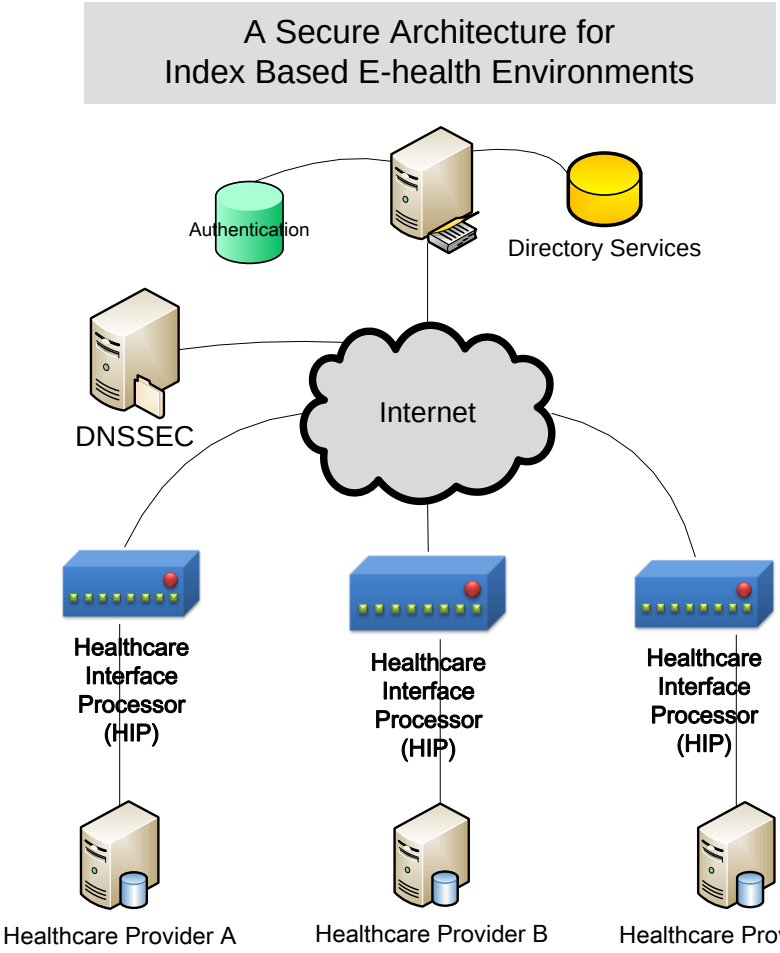


Figure 13: Secure Architecture for Index-Based E-health Environment

The Index System, a centralised facility run at a national level, should be built on a high-trust computer platform to perform authentication and indexing services. The design rationale underlying HIP, a resilient and qualified facility built on top of a trusted base-embedded hardware and software platform, is to act as a proxy server to establish a secured communication channel connecting to the Index System and for health information exchange between healthcare providers. This design could isolate a potentially hostile or compromising system connected to the national e-health network. Wherever a connection to the national indexing system is required, a HIP facility has to exist in some form.

Generally, health information is stored across a number of different health information systems. A national Index System must be available for the provision of directory services to determine the distributed locations of the source systems holding the related health records. This architectural model

draws on important lessons from the Internet's Domain Name System (DNS).[51] This approach embraces the hierarchical and distributed nature of DNS, and defines the required components for a secure architectural design in a national e-health scheme. This architecture also mandates that participating healthcare providers need to adopt a high-trust interface module, the proposed HIP, as the application proxy to connect to the Index System, as well as to link to other health information systems.

A first point of contact in any Index System must itself be verified for authenticity and integrity. In Internet terms, the client system must be certain that it is connected to the correct Index System and not to some fraudulent system or via some intermediate node point capable of monitoring all traffic. A fundamental security issue must therefore be addressed, viz. the veracity of domain names. Trusted domain name resolution services are a critical element in the overall trusted architecture of any index-based healthcare system to combat attacks on the system, such as name resolution cache poisoning, and traffic diversion/monitoring attacks. This security architecture not only provides an indexing service, but also incorporates a trusted name resolution scheme for the enforcement of security in communicating with the authorised Index System.

This research concentrates on the Australian national e-health environment from a security perspective. However, this proposed architecture could be equally applied to any distributed, indexed-based healthcare information system involving referencing of disparate health data collections or repositories.

8.4 Implementation Decision

This section describes the purpose and scope of the development of the test vehicle, as well as the decision made as to the selection of software development tool sets.

[51] RFC 1034 provides an introduction to the DNS functions and protocol for standard data and query types.

8.4.1 Purpose for the Prototype Development

The primary objective of this implementation has been to determine the parameters needed for an appropriate evaluation of any index-based, e-health system project. To date, our research has identified the normal and obvious parameters of the need for optimised performance, coupled with acceptable levels of system security. In fact, this test vehicle indicates a number of additional parameters that need to be considered in any large-scale experimental design, including:

- Clarity and comprehensibility of the overall architecture and allied specifications to enable ready development of prototype systems;
- The need for evaluation of the level of education, training and expertise required by ICT professionals to create and manage such systems; and
- Determination of the guidelines for the creation and assessment of experimental information systems and the associated configurations chosen for the development of such systems.

These three parameters were readily determined even though the experiment performed was of a minimal nature.

8.4.2 Prototype Scope

This proposed architecture concerns the development of a secure architecture design to facilitate patient information sharing and data collection via a national Index System. For demonstration purposes, this paper describes a test environment that consists of a simulated single national Index System and three participating healthcare organisations.

The national Index System in the test environment performs fundamental services, including authentication and directory services. It provides basic authentication services to verify the identity and credentials of healthcare providers; nevertheless, the focus of this paper is to demonstrate the operation of the indexing services themselves. For test reasons, we have used a conventional username/password authentication mechanism. This

module, however, will allow for the incorporation of token-based authentication mechanisms as required. The experimental Index System will provide lookup index referencing to the healthcare service requesting-entity to locate the healthcare information stored at various locations. The Index System facilitates the healthcare service entities in their need to deposit index references for patient records on the Index System.

One healthcare service entity simulates a role of a service requesting-entity, referring as the entity that uses a service provided by another entity. The other two healthcare entities act as service-providing entities that offer health information to another entity.

8.4.3 Selection of Software Development Tool Sets

Since open-source software has risen to great prominence, we have acquired software development tool sets for this prototype based on the concept of open-source technology development. The particular software has been chosen against the contexts of reliability, sustainability, performance, efficiency, accessibility, security, portability, interoperability, total cost of ownership, and maintenance. The selected software development tools are listed in Table 8:

Web Service Framework	Data access connection management (interface)	JNDI
	Web Services Description Language (WSDL)[52] converter	Axis2
	Web Server	Tomcat
Programming Language		Java
Database Management System (DBMS)		Derby
Operating System		Ubuntu

Table 8: Development Tool Sets

8.5 Prototype Structure

Figure 14 illustrates that the prototype structure consists of one national Index System and three participating healthcare entities managing their own healthcare information systems. The Index System is a centralised system run at a national level providing authentication and indexing services. Of the

[52] WDSL is used to describe how to access network services in XML format. More detail is available at http://www.w3.org/TR/wsdl#_introduction, viewed 17/02/2010.

three healthcare service entities, one plays the role of a service-requesting entity, and the others act as service-providing entities.

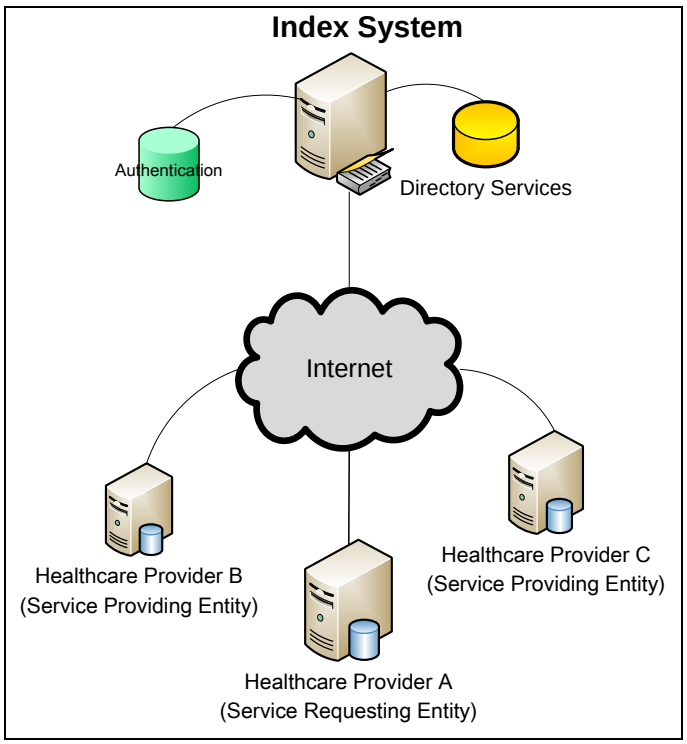


Figure 14: Prototype Structure

8.5.1 The Simulated Index System

Generally, health information is stored over a number of various incompatible health information systems. Indexing services must be available for the provision of directory services to maintain location information for the source systems holding the related health data. The main functions of the Index System should include: (a) authentication services; and (b) publication and discovery healthcare to information services. As various healthcare organisations may have their own specific access to authorisation requirements and processes, privilege management is performed by service providers locally.

In the prototype, the Index System links to an authentication database and directory service repository. The interface used to access the directory services of the Index System is a WSDL interface implementation. The Index System is constructed on Ubuntu and deploys a Web Services stack including:

- Tomcat Web Server, which acts as an enabling platform for the implementation of Axis2 and JNDI;
- Axis2, which acts as a Web Services engine for generating and implementing healthcare applications on a Web Services platform consistent with WSDL specifications; and
- JNDI, which is deployed to manage data connections between the healthcare applications and the DBMS.

For the technical implementation of directory services, each participating healthcare organisation in the national e-health scheme is required to submit its service locator information to the Index System. The submitted information includes the organisational healthcare provider identifier system Uniform Resource Locator (URL), and associated public key. When a new patient record is created on the health information system, the health information system will send an index reference for the new patient record along with its organisational healthcare provider identifier to the Index System. A lookup operation searches for any entry matched with a patient's Individual Healthcare Identifier (IHI) and returns an aggregated list of service instances. The aggregation list of service instances identifies the target system location and information necessary for service invocation. From a database structure perspective, Figure 15 illustrates two exemplary tables and a view (virtual table) in the directory service database: (a) Service Location; (b) Index Reference for Patient Records; and (c) Service Instance View.

The Service Instance View comprises the query results on the target systems which hold the identified patient's health data aggregated from (a) and (b) above.

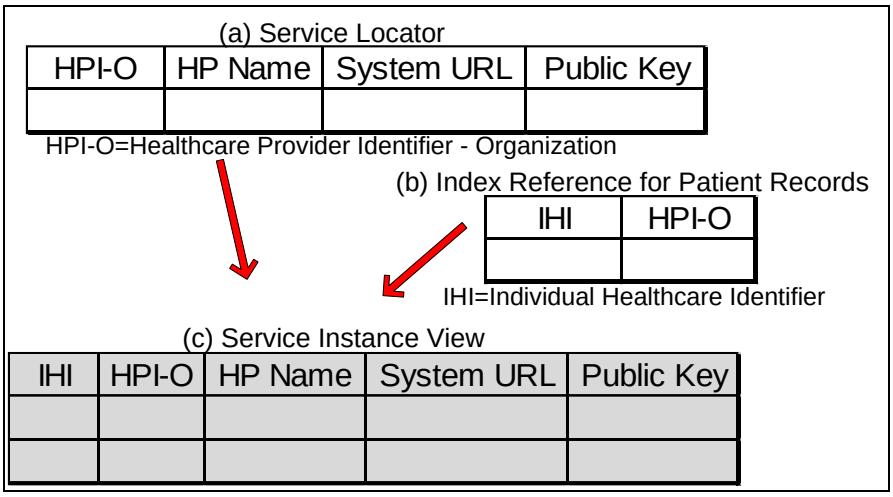


Figure 15: Example of Tables and View of the Directory Service Database

The prototype implementation of the Index System consists of the following system processes to provide authentication, publication, and discovery for healthcare information services:

- Service Locator Registration and Update;
- Index Reference for Patient Records;
- Acceptance of Lookup Query;
- Authentication Operations;
- Resolution of Lookup Query; and
- Delivery Resolution for Lookup Query.

A functional requirement specification provides a description of a particular system process, as well as identifies the data parameters to be entered into that system process. Owing to paper-length limitations, the functional requirement specifications of the system processes listed above are not included in this paper but are available on request.

8.5.2 Virtual Health Information Systems

In general, participating healthcare organisations within a national e-health scheme may use disparate healthcare information systems across multiple platforms. With this test environment, however, we set up the three healthcare organisations to deploy their own healthcare information systems based on the same open-source architecture and software. The main

reason for using the same structure for the three healthcare information systems in the test environment is that each participating healthcare organisation implements a consistent Web Services interface to support service provision and invocation; therefore, interoperability can still be achieved. In the test environment, the health information system implements service provision and invocation in WSDL through support of Web Services interfaces.

Each virtual healthcare information system resides on the Ubuntu operating system and deploys its own healthcare Web services framework, including:

- Tomcat Web Server, which acts as an enabling platform for the implementation of Axis2 and JNDI;
- Axis2, used as a convertor between Java classes and the WSDL format;
- JNDI, used to manage data connections;
- Derby, deployed as the Database Management System; and
- Java applications to invoke and/or provide healthcare services.

A healthcare service entity can play two major roles: as a (i) healthcare service-requesting entity and/or a (ii) healthcare service-providing entity. A service-requesting entity refers to the entity that uses a service provided by another entity. A service-providing entity is an entity that offers a service used by another entity. A service-providing entity can be a healthcare provider, healthcare organisation, or organisation commissioned to provide services for healthcare providers or healthcare organisations.

In the prototype, the healthcare service-requesting system includes the following system processes:

- Request for Service Locator Registration and Update;
- New Patient Creation;
- Lookup Query Handler;
- Reception for Query Resolution; and
- Service Invocation for Patient Data.

The system processes of the healthcare service-providing system in the prototype include:

- Reception for Patient Data Request;
- Token Verification;
- Authorisation Logic;
- Retrieval of Patient Data
- Response to Emergency Access Override;
- Delivery of Requested Patient Data; and
- Notification for Available Health Reports.

Due to paper-length limitations, this paper can only provide an exemplary description of functional requirement specifications from one of the system processes listed above, **Authorisation Logic**.

8.5.2.1 An Exemplary Description of Functional Requirement Specification – Authorisation Logic

The purpose of this system process is to make an access decision upon a patient data request is received at the healthcare service-providing system. The Reception for Patient Data Request process passes the authentication token to the Token Verification process to validate the authenticity of the token. Upon successful token verification, then the requesting healthcare provider's identifiers (i) HPI-O; (ii) HPI-I; and (iii) patient's IHI are passed to the Access Authorisation process. If the access is allowed, the Retrieval of Patient Data process retrieves the request data, or else the Authorisation Logic process produces an "access denied" message.

Not only does the Authorisation Logic process carry the "Sensitivity Label" mechanism outlined by NEHTA [12], but also extends this with "inclusive access" and "exclusive access" provisions to support a finer level of granularity for consent. NEHTA argues that it is necessary to have the "Sensitivity Label" function in place for health data. This enables individuals and their healthcare providers to have the appropriate level of access allowable over sensitive health data. NEHTA suggests two label categories:

(i) “Clinical Care”, and (ii) “Privileged Care.” The “Clinical Care” label normally refers to clinical information that may be accessed by all healthcare providers involved in the healthcare of the patient. Health data labelled as “Privileged Care” can only be accessed by healthcare providers who have been nominated by the patient. NEHTA’s approach uses a coarse granularity for consent. This may not be sufficient to meet the situation where information access control needs to be enforced at a finer level of granularity, however. In contrast, this research represents the following access rules, with the flow chart shown in Figure 16.

The inclusive and exclusive access lists should be defined by patients in conjunction with advice from their healthcare providers when health information is created. Normally, patients make decisions on who is allowed to access their health information. Patients with reduced decision-making capacity may need to compromise some level of their health information privacy to receive the most effective health services.

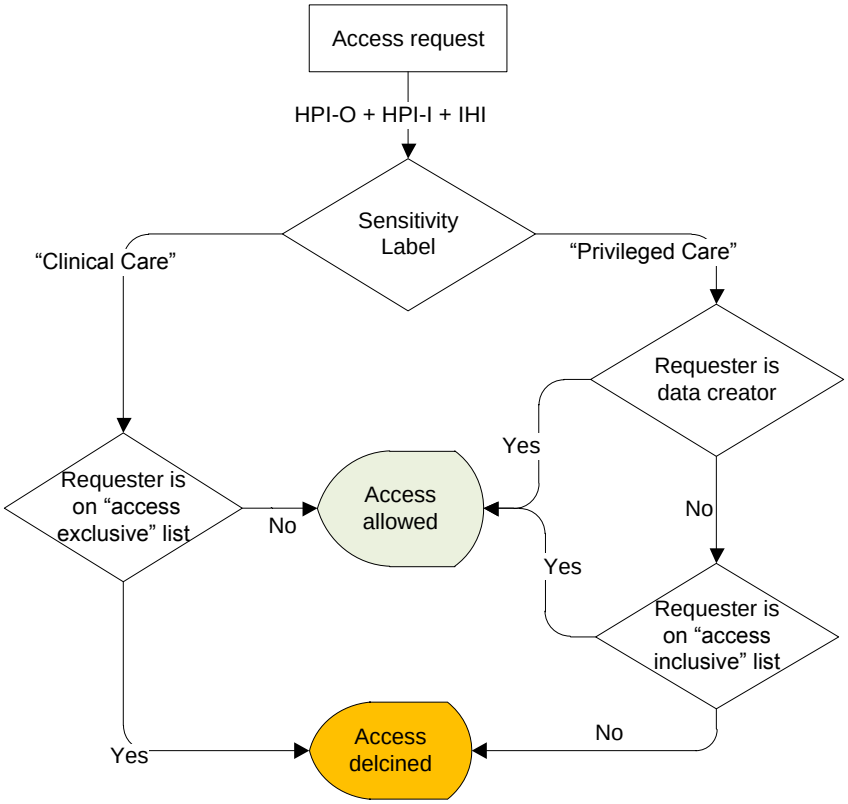


Figure 16: Flow Chart for Authorization Logic

8.6 Key Information Flows

Scenario 1 shows how the proposed system carries out security measures, including authentication, confidentiality, integrity, access control, and transmission security. Scenario 2 demonstrates how the proposed system provides the flexibility of having an emergency override function by switching to a defined emergency policy while activating audit trail functions.

- Scenario 1: A new patient's medical history enquiry; and
- Scenario 2: Emergency override access.

8.6.1 Enquiry for New Patient's Medical History

A new patient, Peter, presents himself for the first time to a medical clinic "A" to seek medical attention. The treating physician in the medical clinic A, David, needs to access Peter's medical history to enable more effective and efficient diagnosis and treatment. It is assumed that David has no prior knowledge that Peter's medical history is located at medical clinics "B" and "C." In this case, the medical clinic A acts as a healthcare requesting entity. "B" and "C" play a role as healthcare service-providing entities. Peter's medical data held at B is labelled "Clinical Care," but Peter's mental medical data held at C is labelled "Privileged Care." David queries the Index System for the source of Peter's medical data. Upon successful authentication, the Index System responds to the request with the source of medical history and signed token for service invocation. David presents the authentication token to medical clinics B and C to request Peter's medical data. As a result, the medical clinic B provides the requested data. The medical clinic C, however, declines the data request because David is not authorised to access Peter's medical data labelled "Privileged Care."

Figure 17 illustrates the key information flows of the interactions between the healthcare requesting entity, Index System, and healthcare service-providing entities with the consequent steps. Meanwhile, this illustration presents how the proposed system architecture can enable secure communications between healthcare providers and the Index System in the national e-health environment.

Note that all request and response messages prior to transmission are signed and encrypted for confidentiality, authentication, and message integrity purposes.

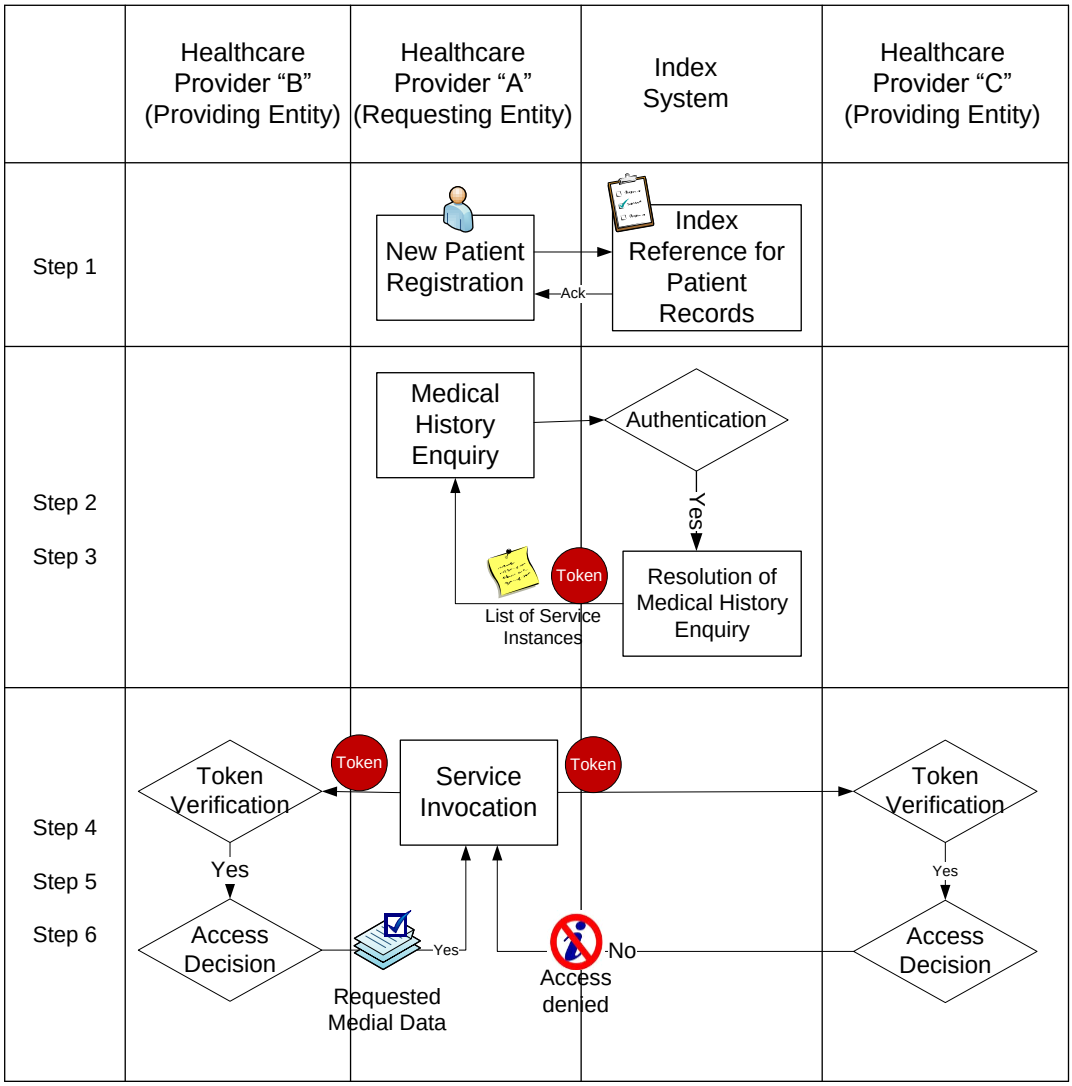


Figure 17: Enquiry for New Patient's Medical History

1 A New Patient Registration

1.1 A new patient, Peter, is registered in A's health information system.

1.2 A's health information system sends a request to enrol this new patient index to the master Index Reference for Patient Records on the Index System.

1.3 Once index reference enrolment to Index Reference for Patient Records on the Index System is successful, the Index System sends an acknowledgement to A..

2 Medical History Source Enquiry

2.1 To be able to query the directory services, a requesting entity must be presented to the Index System with its identity and credentials including Healthcare Provider Individual Identifier and the affiliated Healthcare Provider Organizational Identifier. David logs onto the Index System with A's HPI-O and David's HPI-I.

2.2 Upon successful authentication, David queries the source of Peter's medical history.

3 Resolution of Medical History Source Enquiry

3.1 The Index System searches the master patient index references based on the entry matched to Peter's IHI.

3.2 There are two matched entries found in this case. The Index System then responds with a signed token coupled with the list of the service instance information for service invocation.

4 Service Invocation

4.1 David contacts B to request Peter's medical history with the signed token and other necessary information for service invocation.

4.2 David also contacts C to request Peter's medical history with the signed token and other necessary information for service invocation.

5 Service Provision from the Medical Clinic B

5.1 B validates the signed token and request.

5.2 Upon successful verification, B makes an access decision based on David's profile against Peter's medical data.

5.3 Peter's medical data held at B's health information system is labelled as "Clinical Care", so David's access request is granted.

5.4 The requested data is sent to David.

6 Service Provision from the Medical Clinic C

6.1 C validates the signed token and request.

6.2 Upon successful verification, C makes an access decision based on David's profile against Peter's medical data.

6.3 Peter's medical data is labelled as "Privileged Care" at C's health information system, but David's is not on the "inclusive access" list to access Peter's sensitive medical data, so David's access request is declined.

6.4 The request declined message is sent to David.

8.6.2 Emergency Override Access

There are some cases when medical data must be accessible even in the absence of authorised permission. For example, if the authorised viewer of a patient's case file is not present, but the patient requires emergency treatment, then the availability of the information is more important than its privacy. The service-providing system is programmed to respond to the request for emergency access.

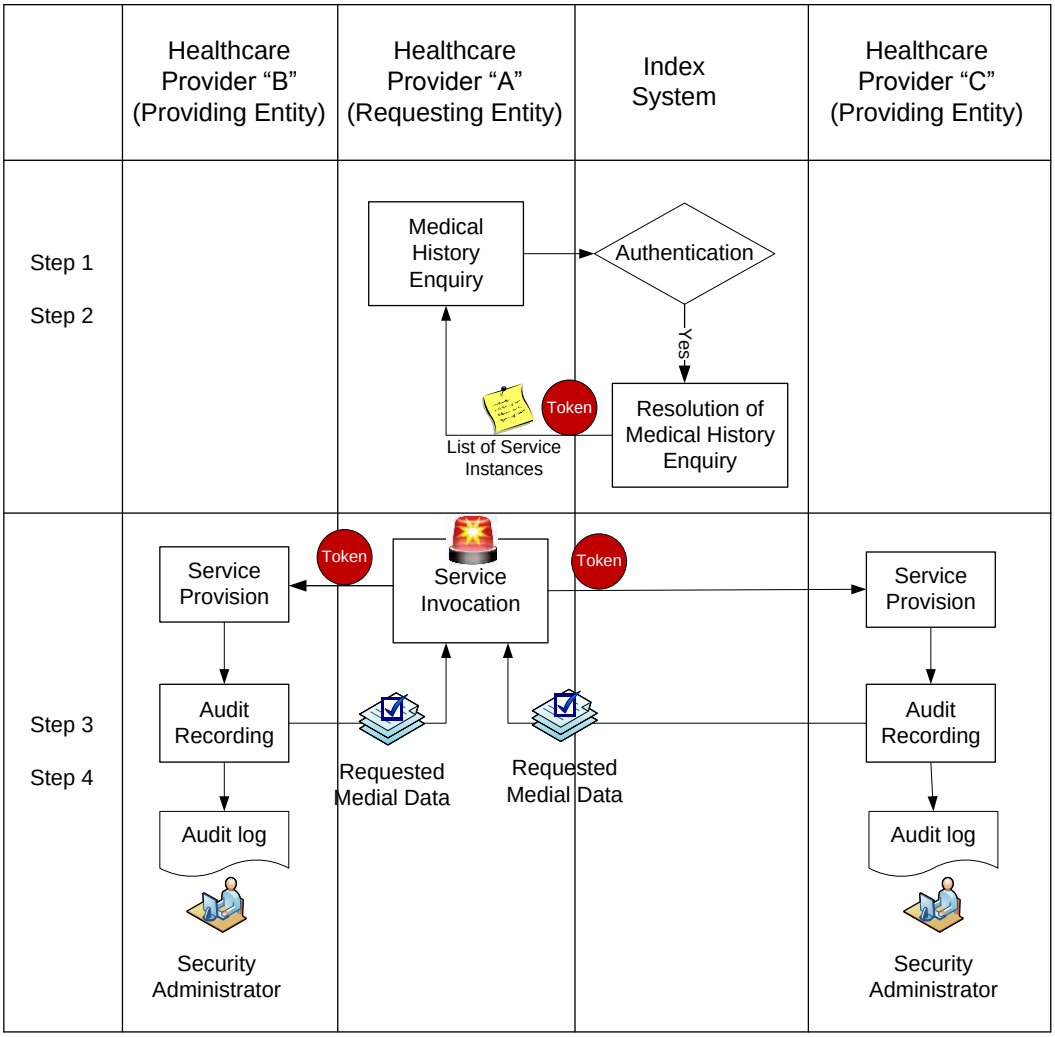


Figure 18: Emergency Override Access

Figure 18 shows the interactions between the healthcare-requesting entity, Index System, and healthcare service-providing entities in an emergency. This illustration also justifies how the proposed system architecture provides the flexibility of having timely access to the requested data with an emergency override function while activating audit trail functions in such circumstances.

Note that all request and response messages prior to transmission are signed and encrypted for security purposes.

1. Medical History Source Enquiry

   The emergency services attending physician queries the Index System for the source of the patient's medical history with the physician's identity and credentials and the patient's IHI.

2. Resolution of Medical History Source Enquiry
   The Index System searches the master patient index references based on the entry matched to the patient's IHI. The Index System then responds with a signed token coupled with the list of the service instance information for service invocation to the requesting entity.
3. Service Invocation
   The service requesting entity presents the signed token to the healthcare service-providing entity for an emergency access to the patient's medical history.
4. Service Provision
   After the healthcare service-providing entity validates the signed token, the process moves into auditing mode without passing through the access decision-making process. To improve privacy accountability and consumer trust through audit trails, the audit trail records who accessed the data and when the data was accessed. The security administrator and patient should be notified of the detection of any unauthorised access.

8.7 Results and Analysis

This prototype project used approximately 288 hours of development effort. This includes times for (i) understanding the architecture and system specifications; (ii) selecting development tool sets; (iii) coding, testing and debugging; and (iv) system documentation. This prototype development was undertaken as a postgraduate student project by working 24 hours per week, completed over 12 weeks during one semester. The prototype developer had three years of practical experience working within the IT industry as an application programmer familiar with Java, JSP, Tomcat, and Oracle database systems. At the beginning of prototype development, to create the healthcare application integration structure based on Web Services, the developer had to self-educate on how to develop distributed Web-based

applications using the Simple Object Access Protocol (SOAP) [53] and WSDL specifications.

Although this experiment has been performed in a minimal manner, the successful completion of this prototype demonstrates the comprehensibility of the proposed architecture as well as clarity and feasibility of system specifications for enabling ready development of such a system. As demonstrated, to create such a prototype system does not require high levels of specialised system development expertise.

This paper describes the technical aspects of the procedures involved in the development of the test vehicle for the proposed security architecture. The result of this paper is useful for providing development guidelines and functional assessment for conforming implementations. This experiment has been to ensure that the system specifications may be readily understood and implemented within a reasonable timeframe and with modest resources. Scalability issues, however, have been not addressed in this experiment.

For the purpose of system analysis, the Australian Government's National E-health Strategy [1] Index Scheme proposal has been used as particular framework in the research undertaken. This research, however, may be more generally applied to any distributed, indexed-based healthcare information systems involving index referencing of disparate health data collections.

The implementation of DNS Security Extensions (DNSSEC)[54] [13-15] has not been incorporated within the test environment, however. For overall trust, DNSSEC would be assumed as a mandatory component to combat the recent increase in DNS cache poisoning and traffic diversion attacks. It is assumed that the first step is to perform the enforcement of trusted communication to the authorised Index System prior to the interactions between the service-requesting entity and the Index System. To achieve this,

[53] SOAP, a platform-independent protocol, normally uses HTTP/HTTPS as the mechanisms for exchanging XML-based messages over networks.
[54] The DNSSEC, through use of Public Key Cryptography, enables DNS "zones" to "digitally sign" the necessary nameserver tables so that, on distribution, such tables can be checked for authenticity and integrity by the receiver.

from a technical underlying process, the health information system should be pre-configured to contact a DNSSEC-capable server to perform a trusted name resolution. This enables the server to defend against false DNS data and to assure that connections are only established with the legitimate Index System.

There is one master Index System and three participating healthcare service entities in the test environment. The Index System is a centralised service implemented at a national level; however, it should be replicated for resilience purposes. This resilient pattern can be seen in the hierarchical and distributed structure of the DNS.

In this test environment, each healthcare service entity connects to the national e-health network system without using the proposed application proxy facility - HIP. It is envisaged that HIP should be used to provide a secured communication channel for an untrusted health information system connected to the Index System, as well as for health information exchange between healthcare providers. Wherever a connection to the national indexing system is required, a HIP facility has to exist.

The authors argue that the load of the national Index System should be relatively lightweight to be able to perform e-health indexing services efficiently. This can mitigate against Index System explosion and traffic bottleneck risks. Such an approach is favourable in a geographically large country such as Australia. To be scalable and to provide effective and efficient operation, the access control and authorisation process is best performed close to where the source system is. This is because each healthcare service provider might implement the service differently based on its own health information system access requirements. Additionally, this prototype system extends the “Sensitivity Label” mechanism outlined by NEHTA [12] with “inclusive access” and “exclusive access” provisions to support fine-granular access control constraints. Further experimentation would be valuable to elucidate requirements in other regimes and architectures.

The United States' *Health Insurance Portability and Accountability Act (HIPAA) 1966* was enacted to encourage a move towards electronic health information systems, while requiring safeguards to protect security and privacy. The Resource Guide for Implementing the Health Insurance Portability Accountability Act (HIPAA) Security Rule [16] provides guidelines for the implementation of the technical safeguards specified in the HIPAA Security Rule. These guidelines cover access control, audit control, integrity, authentication, and transmission security. This research meets all the requirements of the technical safeguards mentioned in this resource guide. One of the access control management activities in this resource guide addresses implementation of the mandatory requirement to "establish an emergency access procedure." This research meets the requirement by providing the flexibility of having an emergency override function by switching to a defined emergency policy in such circumstances, while activating vigorous audit trail functions. In addition, this research ensures that all information prior to transmission is digitally signed and encrypted for confidentiality, authentication, and message integrity.

8.8 Conclusion and Future Work

The successful completion of this prototype development has achieved the following anticipated outcomes:

- The proposed architecture is comprehensible and feasible to enable ready development of prototype systems;
- The creation of such a prototype system does not require high levels of specialised system development expertise, assuming all cryptographic functions are provided;
- The logic model outlined in this paper can be used as development guidelines and assessment for the functionality of conforming implementations; and
- The proposed architecture has met all the requirements of the Resource Guide for Implementing the Health Insurance Portability Accountability Act (HIPAA) Security Rule [16].

This prototype development was not aimed at performance and scalability testing of the proposed architecture. Nevertheless, performance and scalability represent two factors that need to be carefully examined in the development and deployment of any e-health record system. Such analysis is, however, out of the scope and resources of the current project and must be left to future work. It is essential to test the scalability and performance of the proposed architecture against a high order of magnitude in health record infrastructure in the future.

This prototype is developed under a general-purpose operating system that is a "Discretionary Access Control (DAC)" system. It is intended that the system structure be migrated to a more secure platform supporting "Mandatory Access Control (MAC)"-type principles usual in a trusted operating system. Since the indexing services and health information exchange are mission critical, the index system and health information systems must be protected from internal and external threats through the use of modern "Flexible Mandatory Access Control (FMAC)" structures. Under such an operating system, and as distinct from the less secure DAC-based systems, even a system administrator may not have permission to access the health record data. In these systems, there is no "super-user" capable of obtaining access to all system resources at any time. If an individual subsystem is "captured," propagation of exposure will not extend beyond the compromised subsystem itself, a vital concern in any e-health environment, including the "Labelled Security Protection Profile (LSPP)" of international standard ISO/IEC15408.

Part of our future work is to build a HIP prototype. The HIP prototype development is a non-trivial task, which requires sustained collective efforts to incorporate the prescribed provisions, including security, ease of use, flexibility, interoperability, and resilience features. It is intended that such HIP development would involve the production of a number of laboratory prototypes and even the creation of a small production prototype run. The proposed secure and resilient architecture for compliance in index-based e-health environments is therefore timely and critical at present.

8.9 References

[1] Australian Health Ministers' Advisory Council, National E-Health Strategy Summary, 2008. http://www.health.gov.au/internet/main/publishing.nsf/Content/National+Ehealth+Strategy (accessed 1/09/2009).

[2] National E-health Transition Authority, Connectivity Introductory Guide Version 1.1, 2010. http://www.nehta.gov.au/component/docman/doc_download/1041-connectivity-introductory-guide-v11 (accessed 25/10/2010).

[3] M. Morris, PCEHR System Overview, 2011. http://www.health.gov.au/internet/main/publishing.nsf/Content/A30BBA1FBD5C9870CA2578220071D7E1/$File/PCEHR%20System%20Overview%20-%20Speech%20Notes.pdf (accessed 10/02/2011).

[4] National E-health Transition Authority, Endpoint Location Service Implementation Guide Version 1.2, 2009. http://www.nehta.gov.au/component/docman/doc_download/795-endpoint-location-service-implementation-guide-v12 (accessed 30/12/2010).

[5] National E-health Transition Authority, Privacy Blueprint for the Report on Feedback Individual Electronic, 2008. http://www.nehta.gov.au/component/docman/doc_download/587-privacy-blueprint-for-the-iehr-report-on- (accessed 01/09/2009).

[6] National E-health Transition Authority, Connectivity Architecture Version 1.0, 2008. http://www.nehta.gov.au/component/docman/doc_download/624-connectivity-architecture-v10- (accessed 29/07/2010).

[7] Canada Health Infoway, EHRS Blueprint Executive Overview, 2006. http://www2.infoway-inforoute.ca/Documents/EHRS-Blueprint-v2-Exec-Overview.pdf (accessed 15/06/2010).

[8] Canada Health Infoway, A "Conceptual" Privacy Impact Assessment (PIA) on Canada's Electronic Health Record Solution (EHRS) Blueprint Version 2, 2008. http://www2.infoway-inforoute.ca/Documents/CHI_625_PIA_rj13.pdf (accessed 19/05/2010).

[9] B. Blobel, P. Pharow, A model driven approach for the German health telematics architectural framework and security infrastructure. International Journal of Medical Informatics, 2007. 76 (2): pp. 169 -175.

[10] J. Jürjens, R. Rumm, Model-based security analysis of the German health card architecture. Methods of Information in Medicine, 2008. 47 (5): pp. 409-416.

[11] V. Liu, W. Caelli, J. Smith, L. May, M. Lee, Z. Ng, J. Foo, W. Li, Secure Architecture for Australia's Index Based E-health Environment appeared in: The Australasian Workshop on Health Informatics and Knowledge Management in conjunction with the 33rd Australasian Computer Science Conference Brisbane, Australia, (2010) Vol. 108.

[12] National E-health Transition Authority, Privacy Blueprint for the Individual Electronic Health Record, 2008.

http://www.audiology.asn.au/pdf/NEHTA_Privacy_Blueprint.pdf (accessed 9/05/2010).

[13] R. Arends, R. Austein, M. Larson, D. Massey, S. Rose, RFC4033 DNS Security Introduction and Requirements, 2005. http://www.ietf.org/rfc/rfc4033.txt (accessed 07/09/2009).

[14] R. Arends, R. Austein, M. Larson, D. Massey, S. Rose, RFC4034 Resource Records for the DNS Security Extensions, 2005. http://www.ietf.org/rfc/rfc4034.txt (accessed 07/09/2009).

[15] R. Arends, R. Austein, M. Larson, D. Massey, S. Rose, RFC4035 Protocol Modifications for the DNS Security Extensions, 2005. http://www.ietf.org/rfc/rfc4035.txt (accessed 07/09/2009).

[16] J. Hash, P. Bowen, A. Johnson, C.D. Smith, D.I. Steinberg, NIST SP 800-66, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, 2008. http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf (accessed 22/10/2010).

Chapter 9 General Discussion

This chapter provides a concise conclusion to the matters discussed and research results obtained and detailed in this thesis. It also offers suggestions for, and comments on, some future research directions in the area. Extension to the work in this thesis is able to be undertaken towards the implementation of comprehensible, feasible, practical, and trustworthy information systems to enhance the security of, and user trust in, the e-health environment against notable privacy concerns.

9.1 Research contributions

This research clearly indicates that an overall trusted health information system should be implemented with security services and related mechanisms at all levels of its architecture, to ensure the protection of personal privacy and the security of electronic health information. This is in full accordance with the original safety, security, and resilience facilities outlined in the 1980's in the proposed security architecture for Open Systems Interconnection (OSI). From an information security perspective, this thesis proposes the Open and Trusted Health Information Systems (OTHIS), as a broad architecture for the overall health information systems in line with current and emerging policy and legal obligations in many nations. This scheme comprises a set of complementary security modules consisting of three separate and achievable function-based structures developed in a holistic manner. Each module of OTHIS has a specific focus area, as listed in Table 9.

This research has successfully used two proof-of-concept prototypes to demonstrate the comprehensibility, feasibility, and practicality of the HIAC and HIAS components of the overall OTHIS concept. This enables assessment of development guidelines and functionality requirements for trusted health information systems.

OTHIS Module	Focus	Information State
Health Informatics Access Control (HIAC)	Data-centric	Information at rest
Health Informatics Application Security (HIAS)	Process-centric	Information under processing
Health Informatics Network Security (HINS)	Transfer-centric	Information in transit

Table 9: OTHIS modules

HIAC is data-centric dealing with information at rest. HIAS is process-centric dealing with information under processing. HINS is transfer-centric dealing with information under transfer. The relationships between each module have been loosely defined as they are overlapping. For instance, the HIAC fits in the HIAS and HINS modules. Data security through HIAS rests completely upon trust in HIAC and HINS. Trust in network operations through HINS rests completely upon trust in HIAS and HIAC; otherwise the security of messaging becomes futile.

In essence, the specific aims of this study, as stated in Chapter 1, have been answered through five published conference papers, and one published journal article. These papers constitute Chapters 3 to 8 of this thesis. Not only has Chapter 3 investigated national and international e-health management applications and deployment activities, but it also identifies the necessary requirements for the creation of any possible trusted information system architecture consistent with health regulatory requirements and standards. Chapter 4 examines the appropriateness and sustainability of the current approaches for the protection of sensitive electronic patient data in relevant records. Chapter 5 proposes a viable, open, and trusted architecture for health information systems comprising a set of separate, but integrated and developmentally achievable, security control modules. Chapter 6 provides a viable and sustainable approach to the development and deployment of appropriate levels of secure access control management for the protection of sensitive health data. Chapter 7 provides the designs necessary for security controls at Network and Application Levels to protect sensitive health information in transit and under processing. Chapter 8 presents the practicality, feasibility, clarity, and comprehensibility of the proposed security architecture for enabling ready development of secure

index-based e-health systems through analysis of a small experimental prototype system.

9.2 Research analysis

Full security evaluation of any architecture for high-trust healthcare information systems at a national level is a costly exercise. The development of a large-scale prototype or experimental test/simulation system on sufficiently powerful large computer systems, such as supercomputers, is an expensive and onerous undertaking. However, this may be needed to test the scalability, performance, and security enforcement in such very large national infrastructure systems. Such activities have been recognised globally as being outside of the capacity of normal or routine academic research activities, unless such projects are funded through special large research grants and with the availability of necessary supercomputer facilities for simulation purposes.

One relevant “million dollar project” in the 1990’s, the Mach Project [1], was based around the development and testing of an operating system kernel suitable for “next-generation” computer systems. The project was managed and performed by a group at Carnegie Mellon University and was sponsored by the USA’s Defense Advanced Research Projects Agency (DARPA). Another million-dollar project, the Trusted Mach project [2], was also undertaken by Trusted Information System Corporation, again funded by DARPA for the evaluation and testing of a system architecture for high-trust computer systems.

With the research resources and facilities available, the systems architecture proposed in this thesis could only be subjected to very limited experimental evaluation and testing. This testing has mainly involved analysis of the feasibility and implementation needs of the proposed structure. This has used widely-available and understood commodity-level, commercial information system development tool sets and current ICT professional expertise and system development experience. For such a large-scale

information system architecture, questions that could be posed and potentially answered include:

- Is the proposed architecture viable, clear, useful, and comprehensible by ICT professionals?
- Does the creation of such a system require high levels of specialised system development knowledge and expertise?
- Could such a system proposal, in a severely limited and cut-down form, be readily constructed and implemented?

In summary, each of these questions has been answered by this research activity. The architecture has proven to be readily comprehensible by ICT professionals; no specific ICT expertise outside that normally associated with such a professional has proven to be needed. Indeed, a very basic, concept-test-only prototype software system could be developed and demonstrated in a reasonable time at low cost.

As has been acknowledged, a more complete implementation study is well beyond the resources of a university environment and, as mentioned previously [1, 2], a number of prototype healthcare information systems have been developed and tested globally at considerable expense, often exceeding several million US dollars. For example, the National Programme for IT (NPfIT) in England [3], as a ten-year project to provide electronic health record management, is one of the largest public-sector health IT projects in the world. This unprecedented Information Technology project involves the significant investment of £12.4 billion over ten years, with the full cost of this project likely to range up to £20 billion. In 2010, the Australian Government announced the allocation of $AUD466.7 million over the next two years to fund its national electronic record initiative [4].

It must be emphasised that the work outlined in this thesis has been aimed at establishing a broad architecture for security in e-health systems with the identification of necessary subsystems and their associated security parameters. In particular, the thesis has clearly identified the allied problems of:

- Definition of required security functionality;
- Feasibility of implementation and management with an emphasis on required skill sets; and
- Evaluation and assessment of all such systems against agreed industry, national, and international standards.

Traditionally, since the publication of the USA's Trusted Computer Security Evaluation Criteria (TCSEC), known as the "Orange Book" [5], there has been recognition that different levels of system evaluation or assurance exist. As acknowledged by Pfleeger [6], most users and administrators of information systems, large and small, are not information security experts. Pfleeger observes:

"They are incapable of verifying the accuracy or adequacy of test coverage, checking the validity of a proof of correctness, or determining in any other way that a system correctly implements a security policy. An independent third-party evaluation is very desirable: independent experts can review the requirements, design, implementation, and assurance evidence of a system." [6]

In some cases, a formal security definition with/showing a specified level of mathematical rigour may be required. Indeed, at some levels of assurance there may be a need for a "formally verified system design" [6]. Protection mechanisms underlying required security services must, in these specialised cases, be demonstrated to be accurate and themselves capable of being protected. This may involve the creation, and then rigorous assessment, of a formal, mathematical/logical model of the system under study. In practice, such a high level of formal security definition has been practically limited to small subsystems or specialised structures, including cryptographic service modules and a specialised operating system such as the Gemini Multiprocessing Secure Operating System (GEMSOS)[55] [7] which incorporates a high-trust kernel system. Healthcare information systems

[55] GEMSOS, an Operating Systems kernel, has been evaluated at TCSEC A1 class. The GEMSOS kernel has been deployed to protect sensitive national interests on the Internet in high-performance military and intelligence applications.

consist of a number of subsystems and specialised components. As such, to achieve a sufficient assurance level for the defined functionality will be limited in scope and feasibility, possibly attaining Evaluation Assurance Level 4 (EAL4) under the Common Criteria/ISO15408[56] standard. Such evaluation profiles are set out largely as a set of processes and procedures to be followed.

The adoption of an evaluation level of EAL4 appears reasonable for e-health systems and their allied components. This level seems adequate for such systems under any appropriate risk assessment. The EAL4 evaluation level is stated in the Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components [8] as follows:

"EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practises which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

"EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs[57] and are prepared to incur additional security-specific engineering costs."

9.3 Conclusion and future work

Current trends in the ICT sector indicate that information system development and deployment in the healthcare information systems area is fast moving towards use of Web Services structures and even the Cloud Computing paradigm. In this environment focus is placed on security and privacy aspects of patient healthcare records at the Application Level through

[56] The international standard ISO15408: The Common Criteria Toolkit sets a strict guideline for evaluating security policy, program design documents, source code, manuals, and other factors.

[57] With the Common Criteria, the Target Of Evaluation (TOE) is the part of an ICT product, application, or system being evaluated that provides the functionality to counter the threats defined in its security functionality and assurance measures. [This includes its documentation.]

protected electronic exchange of clinical information. This approach has been endorsed by Australia's NEHTA [9]. However, moves towards paradigms such as Service-Oriented Architecture (SOA), Web Services, and Cloud Computing in Information Systems development and usage globally present further major challenges to overall system security and resilience. This applies particularly to the privacy of patient records, where such structures are not based on high-trust operating systems, "middleware," or allied underlying computer and data network systems. Indeed, in these environments the status of basic structures in use may be unknown at the time of development and the time of usage by healthcare professionals. All applications and supporting software which necessarily reside atop an untrusted operating system and allied environments must, by definition, also be considered to be untrusted. A software-based healthcare application can be necessarily no more secure than the subsystems upon which it is built and which are incorporated into its own structure, such as software components. Health information is highly sensitive by nature and its protection is a notable political concern internationally. It is therefore recognised globally that it is critically important to protect the integrity and confidentiality of any such private information from security hazards and allied privacy threats. In this regard, and in this new and emerging information systems environment, risk assessment and analysis continues to play a vital role. It may be reasonably expected that growing privacy concerns will not lessen political and regulatory interest in the area.

This research contends that it is both timely and desirable to move electronic health information systems towards both privacy-aware and security-aware applications that reside on top of a trusted computing-based, Web Services-oriented ICT system environment. Such systems have the real-world potential to satisfy all stakeholder requirements, including:

- The capability for efficient and cost-effective management of modern information structures;
- Adherence to mandatory organisational policies, as well as legislative and regulatory requirements for both healthcare

providers and healthcare consumers with regard to both privacy and security; and

- Flexible operational demands in health information systems.

This thesis emphasises the need for further well-directed research into the application of inherent security-enhanced operating systems and ICT systems structures to provide viable, real-world trusted health information systems. The OTHIS scheme has the potential to fulfil these requirements.

Future work continues on the development of the HINS module within the proposed OTHIS architecture, with the ultimate goals of providing maximum performance and scalability in the healthcare environment. In particular, the development and testing of a prototype HIP unit, as described in Chapter 8, could itself be the subject of another research and development project, with special consideration given to the practical integration of the HIP into national and international Internet infrastructures as well as real-world healthcare information systems.

The HIP prototype development is a non-trivial task, which requires sustained collective efforts to incorporate the prescribed provisions including security, ease of use, flexibility, interoperability, and resilience features. It is anticipated that such a HIP development would involve the production of a number of laboratory prototypes and even the creation of a small production prototype run. This estimation is based upon successful experience in the development and deployment of such units in the banking and finance sector. In this regard, particular note may be made of the successful development, manufacture, and deployment of the Australian Electronic Funds Transfer at Point of Sale (EFTPOS) systems over the last 25 years or more, making use of such hardware/firmware-based products as specialised Hardware Security Modules (HSM), cryptographically-cognisant protocols, and message format conversion units. It is envisaged that the HIP would be subject to specific security functionality needs and evaluation at possibly the minimum requirements of EAL5 under the Common Criteria/ISO15408 standard, in

which Australia participates under the Common Criteria Recognition Agreement (CCRA).[58]

As outlined in Section 3.5.3, future research and development effort needs to be allocated to the problem of developing and testing a Protection Profile (PP) for healthcare information systems. This PP, however, may itself designate additional PPs for vital subsystems that are involved. For example, the protection of patient data privacy normally involves the use of encryption. Thus, a complete evaluation of a healthcare information system may involve the identification of relevant subsystem profiles and a determination of the level of evaluation required, such as beyond EAL4, if deemed necessary. In particular, a PP for the proposed HIP unit could be created in what may be a reasonable time and effort to an evaluation level of EAL5, as mentioned previously in this thesis.

As already stated, modern health information systems may increasingly move towards Cloud Computing involving virtual machines, Web Services, and total dependence upon such Internet facilities and related standards as the Domain Name System (DNS) for the identification of relevant information services. As such, the proposed OTHIS architecture envisages that concerns relating to the trusted nature of the Internet's naming and numbering system, DNS, may be readily incorporated into OTHIS' overall architecture. For example, the defined and standardised Domain Name System Security Extensions (DNSSEC) architecture could be the subject of further research in relation to its likely place in the OTHIS structure and its own security and performance implications.

Recently, Australia's proposed National Broadband Network (NBN) has become one of the most popular topics for discussion in the nation, with analysis from many different points of view including political, economic, and technological factors [6]. The NBN has been seen as providing major healthcare, business, educational, and entertainment advantages. Specifically, the healthcare sector will benefit from much faster network

[58] The Common Criteria Recognition Agreement (CCRA) is available at http://www.commoncriteriaportal.org/theccra.html, accessed 04/11/2010.

connectivity as it delivers online/real-time medical consultations, diagnosis, and treatment recommendations, particularly in rural and regional areas of the country. It is essential that health information systems constructed on this faster broadband network infrastructure be designed and managed in a secure and highly trusted manner to protect sensitive health data in transit. This will boost the confidence of Australian citizens in the security and resilience of e-health applications. If not, malevolent actors could feasibly develop and use illicit means to disclose confidential personal health information, with the resulting breakdown of confidence and trust in any healthcare system deployed over the NBN. The NBN will provide ICT services on a more massive scale and at a much higher speed than seen to date. Exposure to malevolent actors on this scale and with this potential has not been prevalent before. The proposed OTHIS infrastructure is therefore critical at this time.

9.4 References

[1] Carnegie Mellon University, Overview of the Mach Project, http://www.cs.cmu.edu/afs/cs/project/mach/public/www/mach.html (accessed 4/11/2010).

[2] D.P. Juttelstad, NUSC Technical Document 6902: Recommendation Report for the Next-Generation Computer Resources (NGCR) Operating Systems Interface Standard Baseline, 1990. http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA226062&Location=U2&doc=GetTRDoc.pdf (accessed 4/11/2010).

[3] National Audit Office, The National Programme for IT in the NHS, 2006. http://www.nao.org.uk//idoc.ashx?docId=01f31d7c-0681-4477-84e2-dc8034e31c6a&version=-1 (accessed 18/05/2010).

[4] R. LeMay, Budget 2010: e-health scores $466m, 2010. http://www.zdnet.com.au/budget-2010-e-health-scores-466m-339303048.htm (accessed 5/11/2010).

[5] Department of Defense, Trusted Computer System Evaluation Criteria (TCSEC), USA 1983/1985, DoD 5200.28-STD Supersedes CSC-STD-00l-83, dated l5 Aug 83, Library No. S225,7ll, 26 December 1985 1985. http://csrc.nist.gov/publications/history/dod85.pdf (accessed 24/08/2008).

[6] T. Dwyer, Australian Media Monitor. Global Media Journal - Australian Edition, 2010. 4 (1).

[7] Health Level Seven Study Guide. 2008: OTech.

[8] M. Morris, PCEHR System Overview, 2011. http://www.health.gov.au/internet/main/publishing.nsf/Content/A30BBA

1FBD5C9870CA2578220071D7E1/$File/PCEHR%20System%20Overview%20-%20Speech%20Notes.pdf (accessed 10/02/2011).
[9] National E-health Transition Authority, Towards a Secure Messaging Environment, 2006. http://www.nehta.gov.au/index.php?option=com_docman&task=doc_details&gid=63&catid=-2 (accessed 29/09/2010).