12-5-2006

Secure transmission of shared electronic health records: A review

Rachel J. Mahncke
Edith Cowan University

Patricia A. Williams
Edith Cowan University

DOI: 10.4225/75/57b65f9334772
4th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia, 5th December, 2006
This Conference Proceeding is posted at Research Online.
https://ro.ecu.edu.au/ism/80

Secure transmission of shared electronic health records: A review

Rachel J. Mahncke
Patricia A. H. Williams
School of Computer and Information Science,
Edith Cowan University, Perth, Western Australia
rmahncke@student.ecu.edu.au

Abstract

Paper-based health records together with electronic Patient Management Systems remain the norm for hospitals and primary care practices to manage patient health information in Australia. Although the benefits of recording patient health information into an electronic format known as an electronic health record (EHR) are well documented, the use of these systems has not yet been fully realised. The next advancement for EHRs is the ability to share health records for the primary purpose of improved patient care. This may for example enable a primary care physician, with the patient's consent, to electronically share pertinent health information with a specialist, providing timely information transfer and reducing the need for replicated testing. Australia is in the process of adopting a national approach to an integrated health records solution. The Australian National E-health Transition Authority (NEHTA) has released their Interoperability Framework together with specifications and standards for secure messaging in E-health. This is expected to promote an environment in which vendors competing for market share will develop medical applications that are interoperable. With an aging population and the baby boomers preparing for retirement, it is anticipated that these initiatives may indirectly help to reduce the anticipated strain on the health care budget. Anticipated secondary benefits include the collection of de-identified information for public health research and the development of health management strategies. This paper discusses NEHTA's secure transmission initiatives and the resultant security issues related to the transfer of shared EHRs.

Keywords

Medical informatics, e-health, electronic health records (EHR), NEHTA, security.

INTRODUCTION

Paper records together with an electronic Patient Management System remain the norm for hospitals, pathology, radiology, General Practitioners and other health care practitioners to manage patient health information in Australia. Health records aim to store a patients' health information in one place, providing quick access when required. Although electronic health records (EHRs), a computerised format for a paper-based health record, were introduced almost twenty years ago (Bolton and Gay 1995), the use of these systems has not yet been fully realised despite the benefits of recording information electronically being well documented. Electronic records provide additional functionalities over paper-based records, such as the ability to deliver health information in real-time to the point of care, when it is required for the purpose of assisting in clinical decision making and to reduce medical errors (Simon et al 2005). However, the aim of delivering "scalable, flexible, portable, and secure EHR systems" (Blobel 2006) has not yet been fully realised.

The electronic environment makes personal health information available, not only to health care practitioners and hospitals but also to a wide range of "interested third parties such as insurers, employers, laboratories, pharmaceutical companies, government agencies, accreditation and standard setting agencies and researchers" (Murphy 1999). Preserving this private health information for its intended purpose has exposed a new wave of security issues (Williams and Mahncke 2005). Threats to private information in transit include eavesdropping and wiretapping. Many health care professionals are unclear about privacy and data protection laws and what they mean in practice (Meredith 2005). The majority of security breaches are internal resulting from information being accessed by non-authorised members of staff. Reducing the involvement of humans in data could also reduce the number of security violations (Carro and Scharcanski 2006). Additionally, it is estimated that 80% of the total EHR implementation task needs to address the human issues relating to change management (AHRQ 2006).

Three concepts pertinent to any discussion about data security in the health care environment are privacy, confidentiality, and consent (Williams 2005a). Whilst the technology utilised by EHR systems is not new, the lack of global adoption indicates concern for "legal, social, behavioural and ethical requirements that demand" secure patient information (Pharow and Blobel 2004). Carro and Scharcanski (2006) believe that media attention related to Internet security breaches, has caused health care practitioners to delay the development of resources utilising the Internet. In this regard there are a number of obstacles affecting the adoption of EHRs, such as well publicised information disclosures, flaws in systems and insufficient user training. Further, Carro and Scharcanski (2006) reason that the technology developed for use on the Internet may provide the best opportunity to secure electronic health records.

The next advancement for EHRs is the ability to share health records for the primary purpose of improved patient care and to contain costs (Carter 2000, James 2005). Interoperability was defined in 2005 by the Health Information and Management Society as "the ability of health information systems to work together within and across organisational boundaries in order to advance the effective delivery of health care for individuals and communities". This may for example enable a primary care physician, with the patient's consent, to electronically share relevant health information with a specialist, providing timely information transfer and reducing the need for replicated testing. Australia is in the process of adopting a national approach to an integrated health records solution. The Australian National E-health Transition Authority (NEHTA) has released their Interoperability Framework together with specifications and standards for secure messaging in e-health. This is expected to enable an environment in which vendors competing for market share will develop medical applications that are interoperable, known as shared EHRs. With an aging population and the baby boomers preparing for retirement, it is anticipated that these initiative may help to reduce the anticipated strain on the health care budget. Secondary benefits include the collection of de-identified information for public health research and the development of health management strategies. In order to achieve these anticipated benefits, the infrastructure for secure information exchange must first exist. This paper discusses NEHTA's Interoperability Framework, the proposed Web Services Standards Model in order to enable secure transmission, and the resultant security issues related to the transfer of shared EHRs.

NEHTA

NEHTA is a "not-for-profit company established in 2004 by Australian Health Ministers to develop national e-health standards and infrastructure requirements for the electronic collection and secure exchange of health information". NEHTA's primary target is the public sector; however it expects that EHR implemented initiatives will overflow into the private sector. This is already evident in primary practice where the uptake of EHRs by General Practitioners (private health care providers) is greater than that of public hospitals.

Interoperability Framework

NEHTA currently has related initiatives designed to deliver a secure and interoperable e-health environment. Within this framework, electronic health records will enable authorised health care providers to access patients' health care history, directly from clinical information such as test results, prescriptions and physicians notes. Patients will also be able to access their own health record online. Clinical documentation, such as patient referrals and hospital discharge summaries, will be able to be sent electronically directly between health care providers. The security of this exchange will be via NEHTA's secure messaging initiative. Privacy protection and patient consent are built into the framework (Health*Connect* 2006).

The primary purpose of an interoperability framework is to "develop a shared repository of common standards, processes and information components, as well as methodologies for their use, across a diverse range of health systems in Australia" (NEHTA 2006b). Developed based on open software standards this interoperability framework is expected to allow e-health systems to evolve towards interoperability without being constrained by proprietary software products. The interoperability framework provides the base architecture inclusive of "identifying e-health requirements; specifying e-health technical approaches through products and technologies; testing conformance to interoperability requirements; value assessment; and change management" (NEHTA 2006c).

NEHTA's (2006d) framework has been agreed to by all State and Territory Governments, and will ensure interoperability through common e-health concepts, principles and standards that promote and enable interoperability at the "technology, health information, organisational and stakeholder levels" (NEHTA 2006a). The framework is designed to ensure that systems can be added to when required, and allows health IT systems to be tested and certified as being compliant. Secure messaging is just one of the multiple security requirements NEHTA is currently investigating, others are identifiers for patient and health care providers, as well as access and authentication.

SECURE INFORMATION TRANSFER

When a message is generated by the user and transmitted by the application software, until it is received by an authorised recipient the data is subject to a range of security risks. These risks are inclusive of standard security protections relating to hardware, software, human interventions, natural disasters, network issues and logical problems (Farley et al 1996). Clinical information must be transferred securely and like other types of secure transmission must include identification, authorisation, authentication, confidentiality, integrity and non-repudiation. Protecting the data in transit is subject to the same security threats as required for other sensitive data; data may be subject to loss, late delivery, damage, or attack. NEHTA's initiative relating to Identity Management addresses the issues of trusted digital relationships; message integrity, non-repudiation and user authentication. The new Medicare smartcard due to be rolled out across Australia, is in part an enabling technology whereby once user identity is assured then secure transmission can follow.

EHR Issues

The traditional paper-based systems had its own set of security issues including unauthorised access, such as a patient file being viewed and photocopied by an unauthorised person. If unnoticed this breach in security would never be known. Accordingly the electronic storage of private medical information implies a new set of security issues different from the paper-based systems. Previous research by Williams (2005a, 2005b) discusses the threats to medical data in the electronic environment and the risks that should be assessed; however these concerns need to be expanded when considering shared EHRs. The security of medical data comprises of authorised accessibility, which in the medical field relates to confidentiality and privacy; authorised modification affecting the integrity and misuse of information; and accessibility and availability of the data at the time it is required (Williams and Mahncke 2005).

These concerns bring medical data into the same sphere of risk as other networked data, however arguably with added complexity and significance due to the nature of the data itself. Laptops and handheld computers are increasingly powerful, portable and wireless, allowing consultant expertise to be brought directly to the patient's bedside. The capability of networks and the Internet to transfer large amounts of information reliably and securely is also increasing. Soon we will be able to receive more types of data, such as x-ray film and real-time video, over the regular Internet at higher transfer rates. The infrastructure of the Internet is also improving, which will improve the quality and usability of video images on this medium. This has meant that more applications for medicine are being developed (Williams and Mahncke 2005). The protection of personal data in a connected world defaults not so much to high-tech applications or hardware, as to careful management of staff and relatively common techniques to ensure the simple, frequent risks are catered for. The determined criminal or government agency will get access regardless, but what matters to doctors is making sure that we take care of the data we collect about patients in a manner appropriate to the twenty-first century (Williams and Mahncke 2005).

Although EHRs have many benefits these can be compromised if security is not assured when health information is transferred over public and private networks. Systems need to be in place to assure that the data once received is identical to the data that was sent. “Unprotected EHRs can be hacked by identity thieves or stolen in bulk” and insurance companies or employers can make decisions based on this information (Sharpe 2005). Additionally, health information can be mined for data and misused for the purpose of marketing health related products tp patients (Sharpe 2005). Further complications emerge when the protection enforced by one health care provider differs from that enforced by another to whom the record has been transferred. Routine EHR security policies, such as administrative, physical and technical requirements need to be implemented for interoperability to succeed. Additionally, patients need to feel confident that their consent to share health information is sufficiently protected, both technologically and legally.

Current EHR Implementations

The NEHTA proposed secure messaging solution for Australia is different from that being implemented in other Western countries such as the United Kingdom, New Zealand, Denmark and the United States of America. The National Health Service (NHS) in the United Kingdom’s (UK) is responsible for providing health services to the general public (NHS 2006a). UK taxpayers have borne the cost of implementing an internal network ‘spine’ or backbone dedicated to deliver services across the UK. The spine, known as N3, is based on a messaging “hub” approach utilising broadband services from one provider. It is anticipated that by 2010, the UK will have a fully interoperable and secure EHR network in place able to service an estimated 60 million patients whose information is expected to be captured into the system. This is the boldest and most advanced implementation of EHRs to date and the world is using this implementation as a yardstick for future developments and for lessons to be learned. The cost of implementation for Australia will be borne by the organisation, either the hospitals or private medical practices, which has slowed the adoption of EHRs. Table 1 below lists these countries and the target deployment dates for the implementation of EHRs.

Table 1: ***National EHR deployment programmes*** *(OpenClinical 2005)*

Country	Program	Target Deployment Date
Australia	Integrated Health Record and Information System - part of NEHTA. An opt-in system with national trials underway.	To be advised
Canada	National program for a pan-Canadian electronic health record – a major part of Canada Health Infoway	50% of the population by 2010
Denmark	Implementation of electronic health records in hospitals, community health care and general practice.	2003-2007
England	Care Records Service (CRS) for England: a major part of NHS Connecting for Health	60 million records by 2010
Finland	Implementation of national interoperable electronic patient records	2007
France	Dossier medical personnel (DMP) – personal health record	By July 2007 (for all French citizens over the age of 16)
Germany	Current work concentrates on the implementation of electronic health cards for all by 2006. Development of interoperable electronic medical records is expected to follow.	To be advised
Hong Kong	Introduction of a patient-held medical record system in all General Out-patient Clinics (Hong Kong Hospital Authority initiative).	2007
Japan	Part of the eJapan Priority Policy Program. Implementation of electronic medical records in public hospitals nationwide	To be advised
New Zealand	Health Information Strategy for New Zealand (HIS-NZ), 2005. EHRs will be “distributed at local, regional and	HIS-NZ has discounted a single national repository EHR for all

	national levels, with most detailed information about a consumer kept locally”.	an individual’s identifiable health information.
Singapore	EMR Exchange (EMRX) - Initiative by the Singapore Ministry of Health and the two public health care clusters to share information held on EMRs across all public hospitals and polyclinics. Development of a Personal Health Record.	From April 2004
USA	A major part of the Health Information Technology Plan. "Participation by patients will be voluntary."	Interoperable EHRs for "most” of Americans 250 million citizens by 2014.

NEHTA’S MODEL TO SUPPORT SECURE COMMUNICATION IN E-HEALTH

The majority of electronic messaging in health is currently point-to-point (NEHTA 2006c). This is evident in the area of pathology where 55 million electronic messages per annum are currently delivered within Australia (NEHTA 2006). Laboratories have installed proprietary software onto the clinicians’ desktops in order to enable them to view a patients pathology results. This has created a situation where software and standards from multiple vendors has meant an increase in configuration and support issues. This has given rise to secure messaging providers such as Mirapoint.

NEHTA has recommended the use of Web Services (WS) specifications for application-to-application secure messaging as Australia’s secure messaging solution. The model discussed in this section is NEHTA’s solution for secure messaging addressed in the Interoperability Framework, and is the proposed solution for content interchange in Australia, in order to support secure communications of health information (NEHTA 2006a). The technical details of this recommendation are discussed in this section.

Standards and Specifications

NEHTA (2006a) has identified two main standards and related specifications that are needed to enable the sharing of EHR information:

- **Shared EHR Architecture Standards** for specifying the content and logical structure of Shared EHR information and its relationship to clinical concepts, such as Service Oriented Architecture (SOA), and

- **E-health Information Interchange Standards** for specifying the format (syntax and representation) of Shared EHR information for interchange between e-health systems.

Figure 1 illustrates the complexity of the proposed Australian shared EHR standards which provides a framework that will support the capture of health information as shared EHR metadata (NEHTA specifications). Details of how shared EHR information is represented for sharing between e-health systems. Other e-health infrastructure needed to underpin shared EHR implementation is also illustrated for completeness. (NEHTA 2006a). Secure messaging and interoperability form part of the infrastructure of the proposed standards.

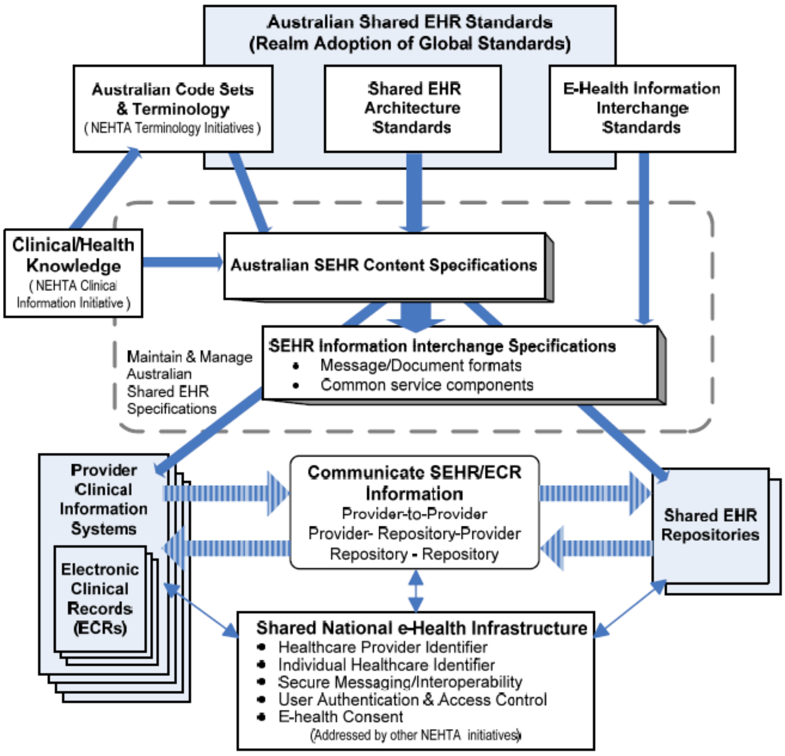
Australian Shared EHR Standards
(Realm Adoption of Global Standards)
Australian Code Sets & Terminology
(NEHTA Terminology Initiatives)
Shared EHR Architecture Standards
E-Health Information Interchange Standards
Clinical/Health Knowledge
(NEHTA Clinical Information Initiative)
Australian SEHR Content Specifications
SEHR Information Interchange Specifications
Message/Document formats
Common service components
Maintain & Manage Australian Shared EHR Specifications
Provider Clinical Information Systems
Electronic Clinical Records (ECRs)
Communicate SEHR/ECR Information
Provider-to-Provider
Provider- Repository-Provider
Repository - Repository
Shared EHR Repositories
Shared National e-Health Infrastructure
Healthcare Provider Identifier
Individual Healthcare Identifier
Secure Messaging/Interoperability
User Authentication & Access Control
E-health Consent
(Addressed by other NEHTA initiatives)

Figure 1: Standardising Australian Shared EHR information (NEHTA 2006a).

The EHR architectures that are "open, user-centric, user-friendly, flexible, scalable, and portable" will enable applications in health information systems and health networks that will support development to meet future demands (Blobel 2006). Accordingly, this model was derived from OpenEHR specifications in conjunction with the Health Level Seven (HL7) v3 standards.

Web Services

NEHTA recommends the use of web services to support secure communications in e-health. The World Wide Web Consortium (W3C) defines a web service as a "software system designed to support interoperable machine-to-machine interaction over a network". The recommended web services standards model is shown in Figure 2. This model incorporates Quality of Service (QoS), messaging, transport and description standards. QoS refers to the guarantee that the network can meet the required traffic demands (Carr and Snyder 2007). QoS includes overseeing the secure transfer of [Extensible Markup Language] XML documents (NEHTA 2006d) by incorporating Web Services (WS)-Security. WS-Security has security features in the header of a SOAP XML message which supports various security formats as well as non-repudiation which is required in the health care environment. WS-Security offers various security options such as "preserving the confidentiality and integrity of messages through the use of authorisation, encryption and digital signatures" (NEHTA 2006). This is effective for trusted communication over public networks as it ensures that the message is secure instead of relying on the security of the transport mechanism. Additionally, NEHTA recommends WS-ReliableMessaging a standard for ensuring that messages are delivery reliably between application systems, even if messages are lost, duplicated, or reordered (NEHTA 2006d).

The recommended messaging standards include WS-Addressing, SOAP, MTOP and XOP as depicted in Figure 2. WS-Addressing provides a "transport-neutral mechanisms to address Web services and messages" (World Wide Web Consortium, 2002). Simple Object Access Protocol (SOAP v1.2), is the standard protocol for Web services and provides the communication framework for secure messaging, inclusive of exchanging messages in a "decentralised and distributed environment" (World Wide Web Consortium 2002). Additionally it defines how messages are represented using XML and is able to "support different types of payloads, behaviours, and interaction patterns" (World Wide Web Consortium 2002).

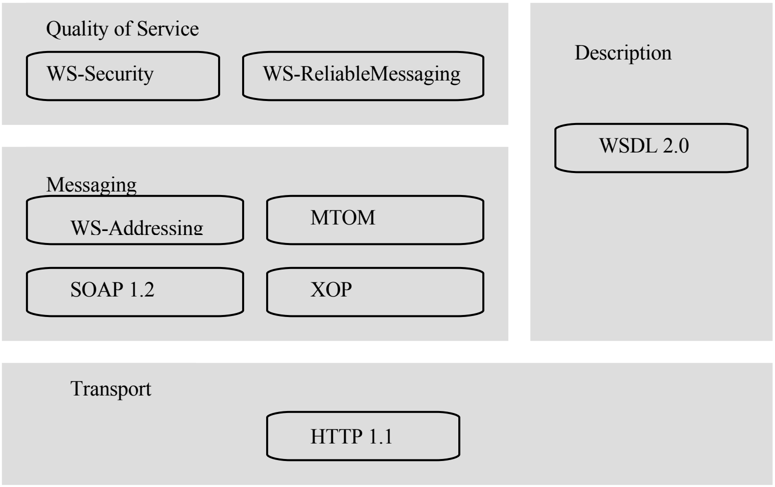

Figure 2: NEHTAs recommended Web Services standards Model

DISCUSSION

In a simplified format, EHR documents are created at the application level; the information through a series of processes is packaged and encrypted into data packets, encapsulated with headers and sent via differing routes onto a series of private and public networks. The data packets are transmitted using sound or light waves which are multiplexed meaning that the waves are manipulated to transmit numerous messages simultaneously. Intercepting all message packets in transit is difficult, and therefore interception of messages is more likely to occur at weaker points anywhere between sender and receiver. The challenge is to implement security at multiple stages and levels in order to ensure that the information arrives at its destination unaltered. Secure email and trusted websites use Transport layer Security (TLS) (which has replaced Secure Socket Layer (SSL)), a protocol commonly used to manage the security of message transmission on the Internet which includes encryption and digital signatures (Carr and Snyder 2007). NEHTAs has extensively investigated the secure messaging technologies but has not recommended TSL for the transportation of health information in Australia.

Since shared documents are easier to intercept compared to accessing data from inside a database, XML is affordable to implement and is completely transparent to the end user (Katehakis et al 2001). Additionally Australian health care is utilising the HL7 standard for translating data between health care systems, and can interchange information by encoding HL7 documents in XML enabling increased security. Web services commonly use SOAP-formatted XML envelopes and Koman (2002) believes that SOAP is a good way to package and move data back and forth between applications. XML enables different systems to communicate, therefore allowing medical records to be transported securely across the Internet (Carro and Scharcanski 2006).

CONCLUSION

Australia is in the process of adopting a national approach to an integrated health records solution. This development requires a robust secure messaging model to support its implementation. The primary authority responsible for guiding the development of this infrastructure is the newly formed NETHA, which has proposed that a web services model be used to support the secure messaging of health information. NEHTA has released their Interoperability Framework together with specifications and standards for secure messaging in e-health. This is expected to enable an environment in which vendors competing for market share will develop medical applications that are interoperable. With an aging population and the baby boomers preparing for retirement, it is anticipated that these initiatives may indirectly help to reduce the anticipated strain on the health care budget. Anticipated secondary benefits include the collection of de-identified information for public health research and the development of health management strategies. The convenience of the established infrastructure in Australia makes this a reasonable approach to contain costs and promote availability in regard to secure messaging of health information.

REFERENCES

ARHQ - Agency for Healthcare Research and Quality. (2006) Community clinics: EHR assessment and readiness project, URL http://healthit.ahrq.gov/portal/server.pt/gateway/PTARGS_0_48447_0_0_18/EHR%20Assessment%20and%20Readiness.ppt,Accessed 14 Nov 2006

Blobel, B. (2006) Advanced and secure architectural EHR approaches, *International Journal of Medical Informatics, 75*(3-4), 185-190. Accessed 8 Oct 2005 from ProQuest Database

Bolton, P., & Gay, R. (1995) Review of computer usage among RACGP members, *Australian Family Physician, 24*(10), 1882-1885. Accessed 17 Oct 2006 from ProQuest Database

Carr, H.H., & Snyder, C.A. (2007) Data communications and network security, Boston: Mcgraw-Hill Inc

Carro, S.A., & Scharcanski, J. (2006) A framework for medical visual information exchange on the web, *Comput Biol Med, 36*(4), 327-338. Accessed 12 Nov 2005 from PubMed Database

Carter, M. (2000) Integrated electronic health records and patient privacy: possible benefits but real dangers, *Medical Journal of Australia, 172*(1), 28-30. URL http://www.mja.com.au, Accessed 8 Nov 2006

Farley, M., Stearns, T., & Hsu, J. (1996) *LAN times guide to security and data integrity*, Berkeley: Mcgraw-Hill Inc

Meredith, B. (2005) Data protection and freedom of information, *British Medical Journal, 330*(7490), 490-491. URL http://www.bmj.com, Accessed 8 Mar 2006

Mount, C.D., Kelman, C. W., Smith, L. R., & Douglas, R. M. (2000) An integrated electronic health record and information system for Australia, *Medical Journal of Australia, 172*, 25-27. URL http://www.mja.com.au, Accessed 8 Nov 2006

HealthConnetct (2006) NEHTA. URL http://www.health.gov.au/internet /hconnect/publishing.nsf/Content/nehta-1lp, Accessed 8 Nov 2006

Ilioudis, C., & Pangalos, G. (2001) A Framework for an Institutional High Level Security Policy for the Processing of Medical Data and their Transmission through the Internet, *Journal of Medical Internet Research 3*(2), e14. URL http://www. www.jmir.org, Accessed 8 Nov 2006

James, B. (2005) E-health: steps on the road to interoperability, *Health Affairs (Project Hope)*, pp. W5-26-W25-30

Kelly, G., & McKenzie, B. (2002) Security, privacy, and confidentiality issues on the Internet, *Journal of Medical Internet Research, 4*(2), e12. URL http://www. www.jmir.org, Accessed 8 Nov 2006

Koman, R. (2002) Clay Shirky: What Web Services Got Right ... and Wrong, URL http://webservices.xml.com/pub/a/ws/2002/04/22/clay.html, Accessed 27 Nov 2006

Murphy, G.F. (1999) *Electronic Health Records: Changing the Vision*, Philadelphia: Harcourt Brace & Co

NEHTA (2006a) Review of Shared Electronic Health Record Standards Version 1.0— 20/02/2006, URL http://www.nehta.gov.au/component/option,com_docman/task,cat_view/ gid,130/Itemid,139, Accessed 8 Nov 2006

NEHTA (2006b) Secure Communication in E-Health. Version 1.1, URL http://www.nehta.gov.au/component/option,com_docman/task,cat_view/gid,129/Itemid,139, Accessed 8 Nov 2006

NEHTA (2006c) Towards a Secure Messaging Environment. An E-Health Transition Strategy Version 1.0, URL http://www.nehta.gov.au/component/option,com_docman/ task,cat_view/gid,129/Itemid,139, Accessed 8 Nov 2006

NEHTA (2006d) Web Services Standards Profile Version 1.0, URL http://www.nehta.gov.au/component/option,com_docman/task,cat_view/gid,129/Itemid,139, Accessed 8 Nov 2006

NEHTA (2006e) Interoperability Framework, URL http://www.nehta.gov.au /component/option,com_docman/task,cat_view/gid,123/Itemid,139, Accessed 8 Nov 2006

NHS - National Health Service, (2006a) History of the NHS, URL http://www.nhs.uk/england/ aboutTheNHS/history/default.cmsx, Accessed 8 Nov 2006

OpenClinical, (2005) EMR national deployment strategies and programmes, URL http://www.openclinical.org/emr.html, Accessed 20 Mar 2006

Pharow, P., & Blobel, B. (2004) Security infrastructure services for electronic archives and electronic health records, *Studies In Health Technology And Informatics, 103*, 434-440. Accessed 4 Mar 2006 from MEDLINE Database

Rashbass, J. (2001) The patient-owned, population-based electronic medical record: A revolutionary resource for clinical medicine, *The Journal of the American Medical Association*. *285*(13), 1769. Accessed 7 Sep 2005 from ProQuest database

Sharpe, V.A. (2005) Privacy and security for electronic health records, *The Hastings Center Report, Health Module, 35*(6), 3. URL http://www.medscape.com/viewpublication/ 1164_index, Accessed 5 Nov 2006

Simon, J.S., Rundall, T. G., & Shortell, S. M. (2005) Drivers of Electronic Medical Record Adoption Among Medical Groups, Accessed 30 Mar 2006 from Ingentaconnect Database

Williams, P.A.H. (2005a) The underestimation of threats to patient data in clinical practice, *In 3rd Australian Information Security Management Conference*. [CD-ROM]. Edith Cowan University, Perth, WA: School of Computer and Information Science

Williams, P.A.H. (2005b) Physician secure thyself*, In 3rd Australian Information Security Management Conference*. [CD-ROM]. Edith Cowan University, Perth, WA: School of Computer and Information Science

Williams, P.A.H., & Mahncke, R. J. (2005) A new breed of risk: Electronic Medical Records Security, *Paper presented at the 6th Australian Information Warfare and Security Conference*, November 24-25, 2005. Melbourne, Australia

Williams, P.A.H., & Mahncke, R. J. (2006) Shared electronic health records: a changing landscape for security in medical practice, *Journal of Information Warfare, 5*(2), 61-72. Accessed 17 Oct 2006 from Informit Database

World Wide Web Consortium. (2002) Web Services Activity, URL http://www.w3.org/2002/ws, Accessed 10 Nov 2006

COPYRIGHT