2011

Why Australia's e-health system will be a vulnerable national asset

Patricia A. Williams
Edith Cowan University

Originally published in the Proceedings of the 2nd International Cyber Resilience Conference, Edith Cowan University, Perth Western Australia, 1st - 2nd August 2011

WHYAUSTRALIA'S E-HEALTH SYSTEM WILL BE A VULNERABLE NATIONAL ASSET

Patricia A H Williams
secau - Security Research Centre, School of Computer and Security Science,
Edith Cowan University, Perth, Western Australia

trish.williams@ecu.edu.au

Abstract

Connecting Australian health services and the e-health initiative is a major talking point currently. Many issues are presented as key to its success including solving issues with confidentiality and privacy. However the largest problem may not be these issues in sharing information but the fact that the point of origin and storage of such records is still relatively insecure. Australia aims to have a Personally Controlled Electronic Health Record in 2012 and this is underpinned by a national network for e-health. It is this very foundation that becomes the critical infrastructure, with general practice the cornerstone for its success. Yet, research into the security of medical information has shown that many general practices are unable to create an environment with effective information security. This paper puts together the connections of e-health and the complex environment in which it is positioned. A discussion of how this critical infrastructure is assembled is presented, and the key vulnerabilities are identified. Further, it addresses how security may be approached to cater for this diverse and complex environment. From a national security and critical infrastructure perspective, as medical records are part of society's critical infrastructure, the most effective system attacks are those on the points of highest vulnerability. In our current health system infrastructure those points are the data collection and records retention areas of individual medical providers. Progress towards changing this situation is key to its success.

Keywords

Medical information security, e-health, Australian infrastructure, cyber resilience.

INTRODUCTION

In May 2010 the Australian Federal Government announced it will spend $466.7 million over two years to create a secure e-health record for every desiring Australian. This is a core function of the e-health initiative currently underway in Australia. The objective of e-health is to improve patient care through the use of information technology and electronic communication by connecting individuals and communities across various healthcare service providers (World Health Organisation, 2009). "E-Health should be viewed as both the essential infrastructure underpinning information exchange between all participants in the Australian healthcare system and as a key enabler and driver of improved health outcomes for all Australians" (Deloitte, 2008).

A fundamental aspect of the e-health record is the assignment of individual healthcare identifiers, consisting of 16 digits, to every Australian. This has necessitated associated new federal legislation. Furthermore, to enable the creation of an e-health infrastructure there are many supporting services being established on a national basis. At present many of these will be managed centrally such as the Healthcare Identifiers Service and the National Authentication Service for Health (NASH). This initiative draws attention to another fundamental issue that has been the subject of much debate in e-health, that of privacy and confidentiality. Given the fragmented nature of the development of privacy policy across Australia although underpinned by the National Privacy Act 1988, this has meant a review of legislation at a federal, state and territory level,. Driven by the evolution of the networked environment since 1988 to 2011, and the e-health initiative, this Act is undergoing major review to among other things bring together the incongruent state and territory privacy legislation. In addition, there has been considerable concern over the actual transmission of health information and its security, in the e-health environment this is referred to as secure messaging. However, in the Australian context the term has taken on a broader meaning than simply protection of the content, it also includes the delivery and identification of the correct healthcare destination and patient identification. This has made this area of development of e-health system more problematic to incorporate unique identification, authorisation and message security in one message.

Whilst these are important aspects of the construction of an effective and safe e-health system, the elemental security of a national system needs serious consideration. Consistent with the "systems" approach to security this is a significant undertaking requiring that all components of such a system be individually secure whilst also ensuring consistent and compatible security between components, in order that the resulting infrastructure is

also secure. Complete oversight and security control of such a system is impossible in the Australian context given the nature of Australia's health system. In countries with smaller populations, smaller geographical area and government controlled health services this is more achievable. However, in Australia the mixture of private and public health providers and services results in less overall control and the responsibility for security devolved to individual healthcare provider organisations. Primary care, which includes general practitioners is the cornerstone to Australia healthcare system. As most primary care providers operate as small businesses this poses additional concerns in regard to implementing effective information security measures including internal expertise, a culture of trust and financial constraints. Indeed, research has shown that this section of the health system is particularly subject to these concerns (Williams, 2010; 2008).

AUSTRALIA'S HEALTH SYSTEM

Australian e-health aims to transform individual paper-based systems into a cohesive and effective electronic system within ten years (AHMAC, 2008). This has resulted in a shared healthcare model that includes a Personally Controlled Electronic Health Record (PCEHR). This requires a "nationally consistent system for identifying individuals, providers and organisations" to "support the implementation of a security and access framework to ensure the appropriate authorisation and authentication of healthcare providers who legitimately access national e-health infrastructure, including the HI Service within the Australian healthcare system" and "support secure messaging from one healthcare provider to another by providing a consistent identifier that can be used in e-communication" (Australian Health Ministers' Conference, 2009).

The justification for such a system is demonstrated in terms of the economic benefit from increased productivity and reduced clinical adverse events. Using an e-health model, this is estimated to be between $6.7 billion and $7.9 billion over 10 years (The Allen Consulting Group, 2008). Further, in terms of patient care, it has been estimated that around 10% of hospital admissions are due to adverse drug events and around 18% of medical errors are due to the inadequate availability of patient information (Australian Institute of Health and Welfare, 2008). Currently $660 million per year in hospital admissions are linked to medication errors resulting from poor availability of patient information (Crozier, 2010).

Attempting to connect all healthcare services and providers is a colossal task. The diversity of provider organisations and their existing individual information systems ensures a resultant complex infrastructure. In a predominantly paper-based system, the infrastructure and information is organisationally based and the management of these resides within the remit of each healthcare organisation. In shifting this to a primarily electronic environment, the design of the entire system becomes more complex. This is due in part to the demands of, and need for, additional identification and authentication. In the physical environment, for instance where a patient is in possession of a written referral letter, normal personal identification suffices. Whereas, in the design of an e-health system (in very cursory terms) must include multiple information source nodes (e.g. a primary care provider), health information exchanges, health information repositories, together with indexing services, security services, and web based portals for healthcare providers and consumers.

HEALTHCARE AS CRITICAL INFRASTRUCTURE

Healthcare services are a critical infrastructure sector for Australia (Australian Government, 2010). Interruption to critical infrastructure and the services it delivers or supports, where this is defined by its impact on the societal or economic well-being or its affect on national security, is a serious concern for government. Within the health architecture this includes hospitals, public health communications and transport, and research laboratories and will be extended to the increasing connectedness of Australia's e-health system. Thus Australians will increasingly rely on an interdependent health system for which the impact of potential cyber attacks cannot be underestimated.

Dependency of health on critical infrastructure

A common question is posed about why the health system and particularly an e-health system is critical infrastructure when healthcare is about treating patients. Indeed, from an individual patient perspective, a clinician can still treat a patient in the absence of information about the patient. However, the e-health critical infrastructure it is not about patient care but the structures and information that support patient care and the system of healthcare provision this provides for the community as a whole.

In addition, new avenues for healthcare delivery are being adopted. Globally there exists considerable interest in the use of technology for remote patient-doctor consultations (Daimi & Song, 2010). The inclusion of unique technically based services such as telemedicine using the Internet or similar capacity communications is an attractive proposition for healthcare delivery in Australia. Expansion of normal healthcare services and reliance on the transfer of information, has led to the use of telehealth as part of healthcare services. This is rapidly being recognised as an essential service for Australia. Indeed, in July 2011, Medicare (the national health funding

body) has incentivised the use of telehealth consultations with both one off set up and ongoing use payments (Medicare, 2011). The real-time security of individual consultations is not an insurmountable problem and several professional medical organisations are producing protocols and guidelines to support its implementation. The security of the consultation will not be an issue, however the increasing utilisation and reliance on these services will be. A major infrastructure or end-user cyber incident would render these services non-operational.

Multiple points of vulnerability

The integration of individual systems creates greater system susceptibilities. Such susceptibilities increase with poor intelligence communication ability. Whilst the focus is still on creating the national system and its connection, and whilst security is an integral concern, the methods to share and collate information on security breaches and attacks do not appear on the agenda. However, there has been a substantial increase of security breaches in the medical industry (Privacy Rights Clearinghouse, 2010) and there is plenty of evidence regarding security breaches. Small organisations, which will make up over half of the connections to the national e-health system , are particularly susceptible. Statistics suggest that 83% of small organizations (with less than fifty staff) had an average of 14 and 45 breaches and this rose to 92% of large organisations in 2009. The categorization of the breaches indicates that malware and attempts at network intrusions were the major sources of breaches, with approximately 60% of organisations reporting their occurrence (Infosecurity Europe, 2010). As yet, there is no mandatory reporting of security breaches as no legislative notification laws exist in Australia resulting in a dark figure of security events.

Another issue in the protection of information in the healthcare infrastructure is that health data travels across domains, whereas in areas such as banking it resides within a single domain (Reid, 2010). This creates vulnerability in the semantic interpretation and interoperability of information exchange. Indeed, one reason that Australia's e-health system has been so long in development is because of this interoperability issue.

MORE PROBLEMS THAN SOLUTIONS?

Significant progress has been made in the construction of Australia's e-health system and in the recognition of the security issues it faces. Driven by the commitment to a personally controlled electronic health record by the government, the services which will underpin this including the health identifiers service and the national authentication service for health (NASH) which is used for verifying the authenticity of both patients and healthcare providers and organisations, will become the cornerstone of the interdependent e-health system. Incapacitation of any of these services will halt the transfer of information in the currently proposed structural e-health model. It should be borne in mind that the final structure of the whole system is still a work in progress.

The rapid adoption of newer technologies and large volumes of patient data makes it a challenge for institutions to maintain security and will pose a major challenge for Australia to progress towards the national e-health interoperability. Unfortunately, whilst larger organizations in the health system may have IT or security trained personnel, primary health care providers in Australia do not. Thus the security function falls to staff which creates considerable exposure of the organization to potential security breaches. The Australian Government (2010) report on critical infrastructure resiliency clearly states that coordination and planning are a necessity. At the same time it acknowledges that the private sector owns and controls the majority of the infrastructure. This means that in an environment where independence is promoted, the major concern is national coordination of recovery from a major incident. In our current health system infrastructure those points are the data collection and records retention areas of individual medical providers and progress towards supporting and educating security to these areas are key to its success in protection and system resilience.

At a more granular level, a key point of the e-heath system is at the local computer system where the raw data is collected and usually stored. Indeed, the current status of information security for all the separate parts of the healthcare services and organisations, particularly the frontline healthcare providers such as primary care medical practices, must be compared to the needs of information security in a broader national e-health system. The potential issues that hamper recovery of a national system are central control and oversight on the conceptual level, as well as the poor understanding of security at the end-user level. At the end points this means that individually, recovery would be reliant on the self-sufficiency of each medical practice. However, the ability of these practices to individually and collectively recover is questionable. For the primary care and the specialist sector of healthcare, in fact any healthcare provider organization of small to medium size will have challenges in resourcing security. These include a lack of time, a lack of funding, and a lack of understanding of the potential dangers and appropriate responses to these dangers. In addition, the ability to put in place effective security measures in health care is also affected by an overarching culture of trust and the heightened responsibility of ethical considerations relating to privacy and confidentiality (Williams, 2008).

At present primary care is not being encouraged to take a larger view of their individual contribution to a national e-health system and what responsibility this entails. For these providers the aspects of business continuity and disaster recovery requires more emphasis. The view of recovery needs to be broader and more

emphatic. To this end the National E-health Transition Authority (NEHTA) has put considerable effort into developing a security and access framework (NESAF). This framework is designed to work across the different domains of healthcare and across the multiple services that are being developed to support the e-health structures. In the past year the review and emphasis on the security of this aspect has been given more credibility and recognised as a fundamental aspect of the total e-health project.

CONCLUSION

The national e-health initiative is an important and positive move forward for Australia and the healthcare benefits it can provide. Healthcare service provision and effective management of information is complex which demands a complex solution. Until Australia's e-health system is fully operational, the realisation of both the benefits and the vulnerabilities may not be apparent. However, what is known is that the vulnerability of this national asset is based on the multiplicity of services required, the mix of public and private healthcare providers, the complexity of connections, the level of knowledge and skills in IT and security, and the difficulty in perceiving a comprehensive national system vision. As yet, an overall approach to Australian e-health system in terms of security and resilience has not been clearly defined, particularly in terms of responsibility.

Each individual healthcare provider and organisation system as well as the local, regional and national physical and information services together makes up the national e-health infrastructure. Ultimately Australia's e-health system resilience and sustainability in face of its vulnerabilities will be the ability of this infrastructure to continue to function correctly, even with diminished performance. This could be achievable if it incorporates a level of adaptability including redundancy, by the individual components that comprise the entire infrastructure. Given this diverse, multifaceted, dynamic structure and its complex interactions, together with the non-static nature of threats and vulnerability, what will be required is an overall 'systems' approach to managing the risks, vulnerabilities, controls and recovery.

REFERENCES

AHMAC. (2008). *National e-health strategy*. Retrieved 19 August, 2010 from http://www.ahmac.gov.au.

Australian Government. (2010). *Critical infrastructure resilience strategy*. Canberra: Attorney-General's Department, Commonwealth of Australia.

Australian Health Ministers' Conference. (2009). *Building the foundation for an e-health future: Update on legislative proposals for healthcare identifiers*. Retrieved 19 Apr, 2011 from http://www.health.gov.au/ehealth.

Australian Institute of Health and Welfare. (2008). *Australia's Health.* Retrieved 01 July, 2011, from http://www.aihw.gov.au/publication-detail/?id=6442468102.

Crozier, R. (May 2010). Budget 2010: Feds move on e-health records. *iTnews.* Retrieved 12 May, 2010 from http://itnews.com.au/Tools/Print.aspx?CIID=174428.

Daimi , K. & Sing, J. (2010)..An approach to secure e-visit systems. In H.R. Arabnia, K. Daimi, M.R. Grimaila & G. Markowsky (Eds.) *Proceedings of the 2010 World Congress in Computer Science, Computer Engineering, and Applied Computing - SAM'10 - The 2010 International Conference on Security & Management*, 487-494. USA: CSREA Press.

Deloitte. (2008). *National e-health and information principal committee: Draf national e-health strategy.* Retrieved 07 June, 2011 from http://www.health.gov.au/internet/main/publishing.nsf/content/604CF066BE48789DCA25751D000C15C7/$File/National%20eHealth%20Strategy%20final.pdf.

Infosecurity Europe. (2010). *Information Security Breaches Survey 2010.* Retrieved 05 July, 2011, from http://www.infosec.co.uk.

Medicare. (2011). *Telehealth*. Retrieved 15 July, 2011, from http://www.medicareaustralia.gov.au/provider/incentives/telehealth.jsp.

Privacy Rights Clearinghouse. (2010). *Chronology of Data Breaches.* Retrieved 10 July, 2011 from http://www.privacyrights.org/ar/chrondatabreaches.htm.

Reid, C. (2010). *Electronic Health Records Today*. Retrieved 05 July, 2011, from http://www.econtentmag.com/Articles/ArticleReader.aspx?ArticleID=66661&PageNum=1.

The Allen Consulting Group. (2008). *Economic impacts of a national Individual Electronic Health Records system*.

Williams, P.A.H. (2008). When trust defies common security sense. *Health Informatics Journal,14*(3), 211-221.

World Health Organisation. (2009). *eHealth for Health Care Delivery*. Retrieved 01 July, 2011, from http://www.who.int/eht/eHealthHCD/en/