2010

Is Cyber Resilience in Medical Practice Security Achievable?

Patricia A H Williams
Edith Cowan University

Originally published in the Proceedings of the 1st International Cyber Resilience Conference, Edith Cowan University, Perth Western Australia, 23rd August 2010

IS CYBER RESILIENCE IN MEDICAL PRACTICE SECURITY ACHIEVABLE?

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

Australia is moving to a national e-health system with a high level of interconnectedness. The scenario for recovery of such a system, particularly once it is heavily relied upon, may be complex. Primary care medical practices are a fundamental part of the new e-health environment yet function as separate business entities within Australia's healthcare system. Individually this means that 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. The current status of information security in primary care medical practices is 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 the poor understanding of security at the end-user level currently, and the lack of central control. This means that in this environment where independence is promoted, the major concern is national coordination of recovery from a major incident. The resilience of a medical practice to cope with a cyber-security incident is important. Resuming normal activity within an acceptable time frame may be vital after a major attack on Australia's infrastructure.

Keywords: Medical information security, e-health, Australian infrastructure, cyber resilience, disaster recovery.

INTRODUCTION

Resilience is the ability to recover, returning to an original state, after some event that disrupts this state (Collins Compact Australian Dictionary, 1999). In the true sense of the word it is synonymous with pliable and stretchable: malleable but not breakable. For the purposes of this paper, cyber-resilience considers how malleable medical information security is, and considers its ability to return to a normal functioning state.

Australia has recognised for some time that the increasing demand for health services has driven the agenda to utilise technology to provide quicker and more cost effective patient care. With an aging population, inequities in health care delivery and a problem in access to skilled health workers, the government has had to search for alternative solutions to healthcare delivery. This requires a nationally connected health system to be established and a shift in the culture for Australians to take more responsibility for their own health outcomes. Australia's national e-health system strategy aims to transform a paper-based system into an electronic system within ten years (AHMAC, 2008). Thus we will increasingly rely on an interdependent health system for which the impact of potential cyber attacks cannot be underestimated. Health services are a critical infrastructure sector for Australia (Australian Government, 2010), and incapacity of this infrastructure would seriously affect the social welfare and healthcare of the Australian population.

The paper reviews the state of security in primary care and then takes a broader, national perspective of e-health. A comparison of the security demands of both perspectives is made with particular reference to the resiliency and interdependence in security.

THE STATE OF PRIMARY CARE MEDICAL PRACTICE SECURITY

Primary care medical practice forms the backbone of healthcare in Australia. One in four people visit their doctor every two weeks (NEHTA, 2010c). As the primary providers of healthcare, medical practices function independently as small businesses, although linked to and guided by national expenditure systems. The operational running of medical practices is not a national concern or under direct governmental control. The only provision is that it there are sufficient providers of healthcare to meet the strategic goals for the nation.
Research has shown that the state of security in medical practice is Australia has room for significant improvement ('Information Security; Insecurities plague electronic health care ', 2010; Williams, 2008a). It

must be remembered that security is not the core business for medical practice. Primary care, like many parts of the health system, is time and resource poor with limited knowledge or understanding of information security. They use information technology as a tool and security is a necessary but not vital part of this. It is the lack of knowledge and acceptance of the reality of risk which causes the problem. This sector of healthcare is primarily driven by the professions in regard to its validation and endorsement in all aspects of its operations.

In regard to information security, the Royal College of General Practitioners (RACGP) accreditation guidelines and standards provide a criterion on privacy and one on information security. The stipulations in Criterion 4.2.2 Information Security (RACGP, 2010) are simplistic at best. However, these are vastly improved from the 2005 version. In regard to disaster recovery the guidelines state that

> When a practice uses computers to store patient health information, the practice needs to have a documented plan (a 'business continuity' plan) in the case of an emergency (eg. power failure) in order to protect and save the information stored in the computers. This plan needs to consider all critical areas of practice function such as making appointments, billing patients and providing adequate clinical care. Once a plan has been formulated, it needs to be tested regularly and documented. All practice team members need to be familiar with their appropriate actions for their role within the practice" (RACGP, 2010).

This is a good start yet in reality it means that the practice has a disaster recovery plan that does not address the implications in a nationally networked and connected arrangement. It is also questionable as to the extent that these plans are developed, understood and effectively tested. Most aspects of security at this policy/procedure level are outsourced to third parties or provided as proforma from the accrediting bodies. Thus, they are not specifically developed by each practice and therefore less responsibility is assumed for their contextualisation and application to that particular medical practice. In addition, current disaster recovery plans are focussed on individual practice recovery only. One of the issues with this scenario is that it is left to the individual practice to source and pay for expertise in this area. Of more concern is that the new RACGP guidelines still refer to the General Practice Computing Group guidelines that have not been updated since 2005 (GPCG, 2005). Funding and expertise is needed to rectify this in light of the push for e-health.

NATIONAL PERSPECTIVE ON E-HEALTH SECURITY

Australia embarked on the development of a national e-health system in 2004. This is being implemented by the government funded National E-Health Transition Authority (NEHTA), however its progress to date has been slow. The focus for the national e-health design is secure messaging. This is because the e-health system itself is made up of the connections between health providers and does not constitute a functionally stand-alone information system.

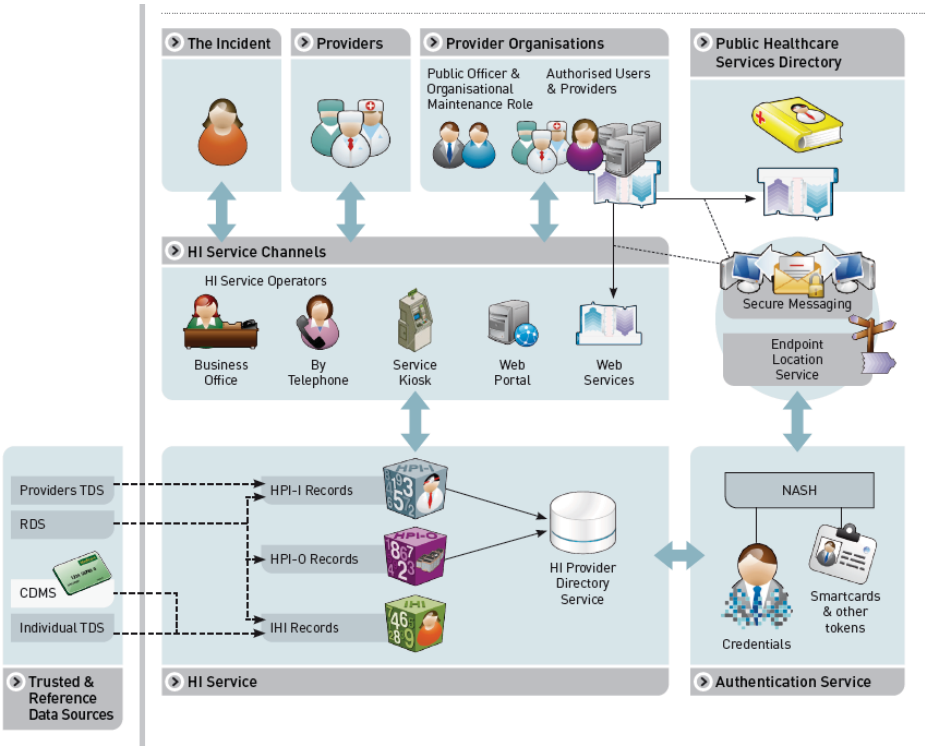

Figure 1. Health identifier (HI) service and its connections (NEHTA, 2009a).

The proposed secure messaging only addresses the secure transfer and transportation of information (NEHTA, 2010a). It is not concerned with security of the initiator/sender of the information and the receiver. In a distributed environment where applications are linked there is increased vulnerability because whilst the transfer of data may be well protected it is the end points (end-user systems) that have significant vulnerability and are open to attack threats. The formulation of this approach has been based on open-source standards and to increase the potential for interoperability because of the structure of Australia health care providers system.

Figure 1 indicates how the information exchange will occur for the national e-health system. The system of data exchange is secure however there is no consideration of the end-points and access points: the HI Service Channels include primary care practitioners, healthcare providers and patients. This is where the vulnerabilities lay. Indeed NEHTA specifically states that the "storage, use and onward transmission of information provided to authenticated and authorised users of the HI Service" is outside its scope of development (NEHTA, 2009b). Interestingly, NEHTA undertook a limited risk assessment of end-user security access, yet only included hospitals and not primary health care providers. This severely limits its conclusions on end-user security issues' considering it is expected that some 500,000 health care providers will participate in the e-health system. It notes that the data collected will inform Participation Agreements and suggestions for security design of third party software. Whilst the HI Service itself will be extremely secure, as yet the aggregation of data and the model for running the e-health system is still in development. Unfortunately, the prime concern has been the secure transfer and communication of information and not the security or resilience of the e-health system as a whole.

Divesting Security Responsibility

The Participation Agreements (NEHTA, 2009b) that form part of the national e-health strategy suggest that responsibility for security is transferred to the individual healthcare provider. It is proposed that these agreements are enforced with responsibility supported by legislation, however no such legislation currently exists. The current baseline security for medical practices is covered by professional accreditation and the Privacy Act. Neither of these is specific, nor does either of them include best practice security. Also, this solicits the question of 'how will it be enforceable with over 500,000 healthcare providers?' This is not to say that each healthcare provider will not implement security to the best of their ability, however at present the level of this implementation is poor and often misunderstood (Wears, 2005; Williams, 2008b).

The security of the e-health system focuses on the use of personal health information and is covered by the overarching statements such as "federal privacy law, state and territory health records, personal information and privacy laws" will be applied and the use of the "healthcare industry codes of conduct relating to patient confidentiality and the security of patient health information" (NEHTA 2010c). This leaves a gap in the overall e-health environment where the national system is vulnerable and its resilience undefined and even unconsidered.

Reliance on Special Technology Services

Around the world there is considerable interest in the use of technology for remote patient-doctor consultations (Daimi & Song, 2010; Griffiths & Christensen, 2007). The reliance on unique technically based services such as telemedicine using the Internet or similar capacity communications is an attractive proposition for healthcare delivery in Australia. Australia is a massive land mass with many remote and rural communities where healthcare delivery is inequitable with those in major urban and metropolitan areas. Telehealth, for states such as Western Australia, Queensland and the Northern Territory, is proving to be a viable and cost effective alternative (Telemedicine, 2010a; 2010b). The government plans to expand the telehealth initiative with funding support and implementation of infrastructure. The real-time security of individual consultations is not an insurmountable problem using cryptography protocols already in place. That is, the security of the consultation will be secure. However the issue is not one of security but of increasingly utilisation and reliance on these services. A major infrastructure or end-user cyber incident would render these services non-operational.

With the issues of limited overarching responsibility for security by NEHTA, the devolvement of responsibility to end-users, and the reliance on technology identified, it is necessary to analyse how this could affect Australia's cyber resiliency in healthcare.

COMPARISON

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. It is an immense task to assume control of a diverse system in the event of a major incident. Thus, the first step in the case of healthcare is to make healthcare providers aware that they actually form part of Australia's critical infrastructure. As Strategy Imperative 2 of the report cites, there is a need to promote an understanding of organisational resilience. However, more than this there is a need for healthcare providers to both recognise and action this imperative. Being aware and understanding are not enough.

The problem with the situation is that the end points of the system are the greatest vulnerability in terms of cyber attack and in displaying cyber resilience. If an attack were to occur on the infrastructure of the national e-health system (the transfer and exchange of information), this would be problematic and cause disruption and delay but the health of individuals could still be catered for. Once the resumption of communications was effected, the data exchange part of the system could be functional again. However, if an attack were to occur that crippled multiple end-points to the e-health system, this could cause major problems for the delivery of healthcare to the community. In addition, without functional end-points there is no e-health system.

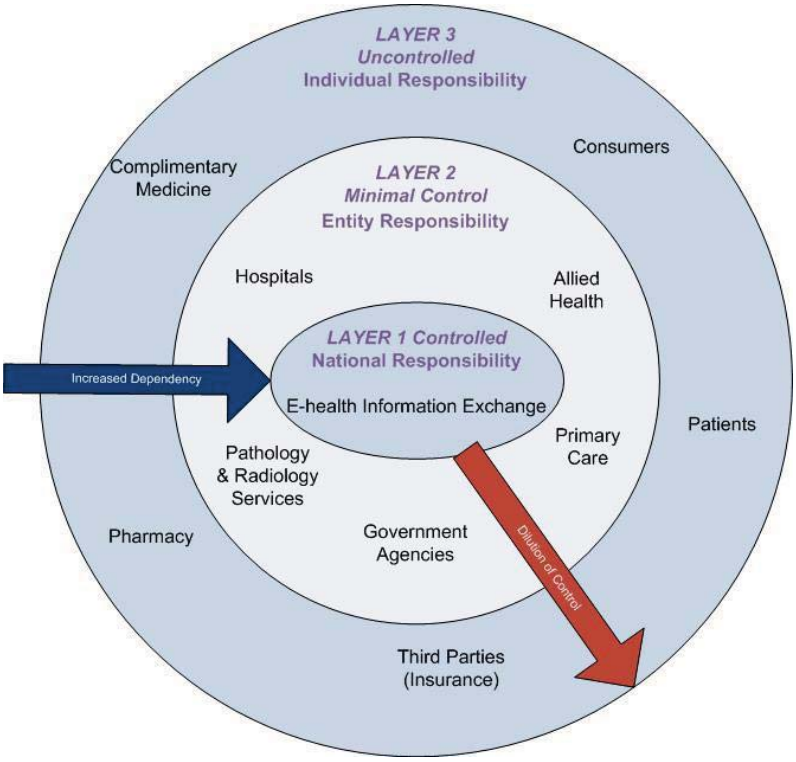

Figure 2. Representation of information security responsibility.

Figure 2 gives an indication of the separation of responsibility within Australia's healthcare environment. Whilst there are levels of responsibility from an entity viewpoint, the dilution of control from the central point outwards poses a dilemma, whilst the dependency increases. The e-health system (layer 1) is dependent on the outer layers (2 & 3) to function. Under normal operating circumstances this system may function well. Any minor interruption will not necessarily disrupt the whole system's functionality. Similarly, any major or minor event in layer 3 is unlikely to significantly adversely affect layer 1. However, a major cyber incident in layer 2 would cripple layer 1 and detrimentally affect layer 3. The situation is complex due to the multiple independent and diverse contributors to the health system, and the indeterminate nature of the boundaries between providers. The layers are no discrete and distinct.

Recognition of these problems is not sufficient. Strategy that incorporates responsibility and coordination of recovery is required. Unless a national approach is taken, Australia is not only vulnerable but is not resilient.

Critical Omissions

There are several issues that should raise significant alarm.

From a national perspective:

- A colossal gap in the development of Australia's e-health system is any acknowledgement of the potential for disaster, business continuity and recovery. There is no mention of it in the NEHTA strategy or operational documents.

- There is no security responsibility for the e-health system as a whole. Therefore no coordinated control function has been defined in the event of a major infrastructure failure or cyber incident.

- The NEHTA documents fall short in guidance and recognition that the providers of the healthcare information may be an area of concern. Whilst this may not have been within the scope of their objectives, it should at least be acknowledged as an issue that would need addressing.

From a primary care healthcare provider perspective:

- Current guidelines are incomplete in information security practices. Despite stated involvement of the RACGP with NEHTA (NEHTA, 2010b) in developing the standards, the updated 4th edition of standards are dangerously deficient in the area of information security (RACGP, 2010).

- 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. The aspect of business continuity and disaster recovery needs more emphasis. The view of recovery needs to be broader and more emphatic.

The issue to be addressed is not that the government should control all layers of the healthcare system infrastructure (Figure 2), rather that there is national recognition of the inherent vulnerability in its construction and use. From a national perspective, security policy and responsibility needs to be given more credence. The possibility of cyber threats occurring and the resultant detrimental impact is real. The very characteristics that have given us the ability to contemplate and develop a national e-health system are also pivotal to its potential destruction. Computing and telecommunications provide the capability and interoperability required that makes the Internet such a success. Yet, it is this accessibility that also causes the insecurity.

What is not considered here is the motivation and ability of individuals or state actors to carry out deliberate attacks on Australia's healthcare system. Whilst this is an important factor with which to drive national strategy, it is not reasonable to base protections on incalculable risks. Given the undefined and unsubstantiated nature of cyber threats, it is better to ensure that the protections exist in the first place.

CONCLUSION

If Australia's future healthcare system is to increasingly rely on the digital environment, with cyberspace as its primary communication method, then potential cyber security issues and disaster recovery must be addressed. The e-health system is a national asset and therefore must be dealt with on a national level. Leaving recovery to individual uncontrolled sections of the healthcare system is insufficient and dangerous. Whilst the protection of the infrastructure itself is within the national security remit, the resulting recovery effort needed in individual healthcare provider businesses will be left to chance. Australia's resiliency of this critical system will be measured by this.

Current research is looking at the issues in the end user environment including the vulnerability of medical software, security governance, and security capability within General Practices. A coordinated and multifaceted approach needs to be adopted quickly if Australia is not to become a fatality in the cyberspace environment. The ability of primary care practitioners to recover as independent entities means that there is no control over how, when or even if, they will recover. Without direct government involvement or some form of coordinated approach the resilience of our health system is haphazard at best and may fail entirely at worst. Australia is vulnerable because of the structure of its healthcare environment. There is no accountability for coordination in the event of such a disaster. The improvements we make in healthcare through e-health connections may also be our greatest vulnerability.

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.

Collins Compact Australian Dictionary. (1999). Resilient. HarperCollins Publishers: Sydney.

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.

GPCG. (2005). *E-health: General practice computing group.* Retrieved 19 August, 2010 from http://www.racgp.org.au/gpcg.

Griffiths, K. M. and H. Christensen (2007). Internet-based mental health programs: a powerful tool in the rural medical kit. *The Australian Journal of Rural Health 15*(2): 81-87.

ITU. (2005). A comparative analysis of cybersecurity initiatives worldwide. WSIS Thematic Meeting on Cybersecurity, Geneva 28 June – 1 July, 2005.

Information Security; Insecurities plague electronic health care. (2010, August). *Information Technology Newsweekly,*285. Retrieved August 19, 2010, from ProQuest Computing. (Document ID:2093445321).

NEHTA. (2009a). *Introduction to national infrastructure services.* Retrieved 19 Aug, 2010 from http://www.nehta.gov.au.

NEHTA. (2009b). *HI service security and access framework.* Retrieved 19 Aug, 2010 from http://www.nehta.gov.au.

NEHTA. (2010a). *Secure messaging fact sheetv2.0.* Retrieved 19 Aug, 2010 from http://www.nehta.gov.au.

NEHTA. (2010b). *National certification capability for e-health: Discussion paper – towards a concept of operations.* Retrieved 19 Aug, 2010 from http://www.nehta.gov.au.

NEHTA. (2010c). *Health identifiers service implementation approach.* Retrieved 19 Aug, 2010 from http://www.nehta.gov.au.

RACGP. (2010). *RACGP Standards for general practices, Draft 4th edition for consultation.* Retrieved 19 August, 2010 from http://www.racgp.org.au/Content/NavigationMenu/PracticeSupport/StandardsforGeneralPractices/4th_edition_RACGP_draft_standards.pdf.

Telemedicine.(2010a,August) New findings from University of Queensland in the area of telemedicine published. *Medical Devices & Surgical Technology Week,*1630. Retrieved August 20, 2010, from ProQuest Health and Medical Complete

Telemedicine (2010b ,June). Studies from Lions Eye Institute provide new data on telemedicine. *Medical Devices & Surgical Technology Week.* Retrieved August 20, 2010, from ProQuest Health and Medical Complete.

Wears, R. L. & Berg, M. (2005). Computer technology and clinical work: still waiting for Godot. *JAMA 293*(10), 1261-1263.

Whitten, P., Buis, L. and Love, B. (2007). Physician-patient e-visit programs: Implementation and Appropriateness. *Disease Management & Health Outcomes, 15* (4), 207-214.

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

Williams, P. A. H. (2008b). How addressing implementation issues can assist in medical information security governance. In N. L. Clarke and S. M. Furnell (Eds) *Second International Symposium on Human Aspects of Information Security and Assurance*, pp. 116-125. Plymouth, UK, Centre for Information Security & Network Research, University of Plymouth.