Sound Foundations: Leveraging International Standards for Australia's National Ehealth System

Patricia A H Williams[1], **Vincent McCauley**[2]

[1] School of Computer and Security Science, eHealth Research Group, Edith Cowan University

[2] Medical Software Industry Association

Abstract

Background: Australia is currently in the process of deploying a national personally controlled electronic health record (PCEHR). This is being built using a combination of international standards and profiles as well as Australian Standards and with specifications developed by the National eHealth Transition Authority (NeHTA). **Objective:** There exists a poor appreciation of how the complex construction of the overall system is supported and protected by multiple international standards. These fundamental underpinnings have been sourced from international standards groups such as Health Level Seven (HL7) and Integrating the Health Enterprise (IHE) as well as developed locally. In addition, other services underlie this infrastructure such as secure messaging, the national Health Identification Service and the National Authentication Service for Health (NASH). **Methods:** An analysis of the national e-health system demonstrates how this model of standards and service integration results in a complex service oriented architecture. **Results:** The expected benefits from the integrated yet highly dependent nature of the national ehealth system are improved patient outcomes and significant cost savings. These are grounded and balanced by the current and future challenges that include incorporating the PCEHR into clincial workflows and ensuring relevant, timely, detailed clinical data as well as consistent security policy issues and unquantified security threats. **Conclusions:** Ultimately, Australia has designed an ambitious yet diverse and integrated architecture. What remains to be seen is if the challenges that the medical software industry and clinical community face in leveraging the political process in order to encourage provider and public participation in ehealth, can be achieved despite the sound underpinnings of international standards.

Keywords

Medical Informatics Computing, Health Communication, Data Sharing, Health Level 7, Electronic Health Records

Correspondence to:

Dr Trish Williams
Edith Cowan University SCSS, JO Bld 18, 270 Joondalup Drive, Joondalup, WA. 6027. Australia e-mail: trish.williams@ecu.edu.au

EJBI 2012; 8(4):50–55

1 Introduction

In Australia there is an undeniable uniqueness to the healthcare environment that has resulted in a complex approach to the development of a national e-health system. It is important to appreciate what these distinct drivers are if there is to be an understanding of the structure and functionality of such an ambitious project. The development and implementation of the Australian national e-health system represents an important and radical change to the healthcare system and critical societal infrastructure.

The uniqueness arises from a number of drivers and characteristics peculiar to healthcare. The drivers in Australia are heavily influenced by the political landscape and the time deadlines imposed by the government. From the perspective of the characteristics of the healthcare delivery environment, the imperative is to have the right data in the right place at the right time, and an urgency driven by clinical need and conditions. Added to this is the complex sequencing of clinical steps and the coordination of parallel patient care, complicated by difficulties with infrastructure and availability of trained personnel across diverse care settings from major cities to remote Aborigi-

nal communities.

This impact of these factors on the applications and software used to delivery and support ehealth is that there is an inimitable complexity of data and documentation, and a labyrinth of data requirements across a distributed system. The distribution is not merely in location but of time and person given the dispersed web of healthcare providers. This environment requires a complex construction of governance because of the public (40%) and private (60%) split in service delivery and due to its multi-tiered, distributed arrangement. This governance structure creates a disjunction between costs and benefits. The electronic age where information, both good and bad, is not in short supply, demands a medico-legal practice of defensive medicine, in addition to the primary prerequisite of medical practice to 'first do no harm'. The need to tame this clinical information tsunami means it is increasingly important to provide effective and readily adoptable clinical decision support. The relevance of these factors to the development of software applications, services, and the supporting information exchange architecture [1] means that developers are wading into a highly complex and contextualised environment. This situation is further complicated by the consideration of privacy and security [2] and the sensitivity about government concentration of personal information.

This paper explores the complex underpinnings of Australia's national ehealth system and the Personally Controlled Electronic Health Record (PCEHR). The basis for using standards and their impact is discussed to preface the analysis of the challenges that such a national system presents to those who have to deliver it – the software industry; those who are to use it - the clinical community; and those who are the consumers of it - the public, and how these challenges create tensions despite the sound foundations that the system is built upon.

1.1 Background to the Personally Controlled Electronic Health Record

Australia, like many countries, is facing increasing challenges in delivering high quality healthcare to an aging population and increases in chronic disease whilst attempting to control spiralling costs [3]. As part of Australia's national health reform Australia is introducing a Personally Controlled Electronic Health Record (PCEHR) [4, 5]. The PCEHR is a primary constituent of the national health reform agenda and as such has been the focus of the development of Australia's ehealth architecture [6]. The PCEHR "aims to place the individual at the centre of their own healthcare by enabling access to important pieces of health information when and where it is needed by individuals and their healthcare providers" [7].

In the Australian healthcare environment there are a number of complementary bodies involved in and impacting the development of the national ehealth system as shown in Figure 1. These include the government sponsored organisations charged with the delivery of the overarching architecture namely National eHealth Transition Authority (NeHTA), the Federal Departments of Health and Ageing (DoHA) and Human Services (Medicare); and the standards and stakeholder communities comprising of national and international standards organisations and technical stakeholders. The national and international standards organisations work underpins the establishment of this architecture such as Health Level 7 (HL7), the International Standards Organisation (ISO) - Health Informatics Technical Committee TC215, Integrating the Health Enterprise (IHE) and Standards Australia (SA) – IT-014 Health Informatics Technical Committee. The technical stakeholders include the Medical Software Industry Association (MSIA) who represent the clinical and supporting system suppliers.

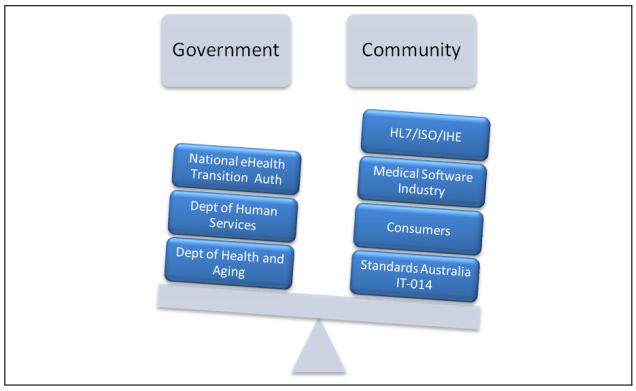

Figure 1: Contributing national organisations and groups in the Australian ehealth standards process.

As with any major government initiative there are inevitable tensions in meeting the needs of the various stakeholders. The tensions have been exacerbated by short politically driven time frames, the enormity of work involved, confusion over leadership roles, the difficulties arising from reliance on a community of volunteer experts to deliver outcomes and key performance indicators for government sponsored organisations. This volunteer community is arguably the ehealth community's most valuable yet undervalued asset. This method of harnessing volunteer experts, who work in the health informatics and related industries, only functions effectively because such people are committed to the outcomes trying to be achieved for Australia nationally. The involvement and collaboration of all stakeholders in Figure 1 is essential to avoid duplication of standards and to obtain engagement and support particularly where the end-user vendor community is bearing a large percentage of the costs. Further, it promotes transparency and harmonisation in a sector that uses multiple models for development, and has a diversity of healthcare delivery requirements. The standards need to ensure that they support all sectors of the healthcare community and do not create unnecessary barriers to innovation and market competition.

2 Standards as a Basis for Systems Development

A standard is an expert consensus document that provides a benchmark for a product or service [?]. Such consensus "represents the best knowledge in the field" and essential contribution by people who are regarded as the technical experts in their field, and in this case are experts in health and health informatics [?]. Standards are practices that are recognized for their quality and can be used as a measure for comparison. Like laws, they need to be monitored and enforced to be effective. Standards provide guidelines for best practice, consistency and interoperability [10] and are an essential feature in a minimally regulated field such as computer and information science. Thus, when this field and the healthcare environment are combined, the requirement for standards is imperative to mitigate potential for safety issues. Further, standards are essential for consistent outcomes to security reusability and end-point security stability, even though the approaches may vary. This is also important as one solution does not meet all the needs.

The use of standards, not to be confused with standardisation, is to facilitate the effective interoperability in communications. One of the underlying drivers for creating uniformity through standards is to address the issues of safety and quality which is of particular importance in the healthcare application environment. Further, standards in software development are beneficial in the ability to reuse specifications from consistent, expert evaluated documentation. Informed, independent and objective professional review also contributes to increased clarity of requirements specification [11]. Further, it contributes to lowering integration costs, fosters vendor innovation and competition with no specific vendor lock-in for users, which are all important factors in the development of a nationwide interoperable system in Australia's free market economy. These are all benefits of using local and international standards where multiple but integrated services are required. This also fosters an independent plug and play approach to software and service integration – a goal of services oriented architecture (SOA).

Designs of formal electronic health records have focused on the integration of intra-enterprise applications. This severely limits the scalability and interoperability required for distributed systems [12]. Thus the move to SOA is attractive, although complex and a major challenge to design on a national scale. There are examples of SOA designs at an organizational level, but few at levels wider than this. What SOA potentially provides is an overarching architectural framework which allows the functionality of multiple competing but complementary services to be brought together. The reuse and enterprise application integration is an attractive proposition supporting modularity and interoperability, using services as the building blocks for development of flexible but reliable system components [13]. In addition, SOA can forge a pathway for migration from legacy systems as it permits software solutions at different levels of technical maturity to effectively interoperate.

2.1 The Australian Experience

As has been shown in other countries, the challenge is to integrate standards nationally and internationally that support the needs of the environment to which they are applied [14]. In order to avoid the case where proprietary developed standards hamper national interoperability, Australia has taken a 'standards based approach' to the development of the ehealth architecture. Further, the collaboration between the government sponsored organisations and the standards development and implementation community in Australian healthcare, as in Figure 1, has been used to enhance interoperability among the multiple stakeholders and the standards making communities. This is important as it has been demonstrated that the numerous standard development organisations themselves may create confusion for standards adopters, namely industry, instead of promoting interoperability [15]. Collaboration at any level is a beneficial objective to pursue, to avoid gaps in requirements and unnecessary overlap of standards and subsequent disparity between them.

In creating Australia's ehealth interoperable environment a number of standards are used including HL7 Clinical Document Architecture (CDA) and Integrating the Health Enterprise - Cross Enterprise Document Sharing (IHE XDS.b) profile, specified for the Australian PCEHR and associated conformant repositories. The standards upon which the Australian ehealth system is based are well established and used internationally. For instance "the IHE IT Infrastructure (ITI) domain addresses the implementation of standards-based interoperability solutions to improve information sharing, workflow and patient care" [16]. It achieves this with the harmonized use of established international standards such as DICOM and HL7 within an SOA framework.

These international standards are core to ehealth interoperability and supporting services such as the National Authentication Service for Health (NASH), Health Identifiers Service (HI), Secure Message Delivery (SMD), Endpoint Location Service (ELS), Health Care Provider Directory (HCPD), Audit and so on. Some have been modified and extended by NeHTA, for instance, the CDA standard has been extended in a manner permitted by the CDA standard but may not result in adoption internationally and may not end up being incorporated into the international standard. At present these extensions are localised to Australia.

2.2 A Service Oriented Architecture for the PCEHR

There is an increasing push to adopt services oriented architectures across organisations [17]. This is partic-

ularly pertinent to the healthcare environment as SOA addresses some of the common problems that healthcare computing faces in a complex work environment with a need for legacy system re-use, and requiring linkage of multiple interfacing systems [18].

Figure 2 provides a representation of how primary services are integrated for the PCEHR, and how they are moving towards a service oriented architecture. This diagram indicates how technical specifications and standards underpin the national PCEHR.

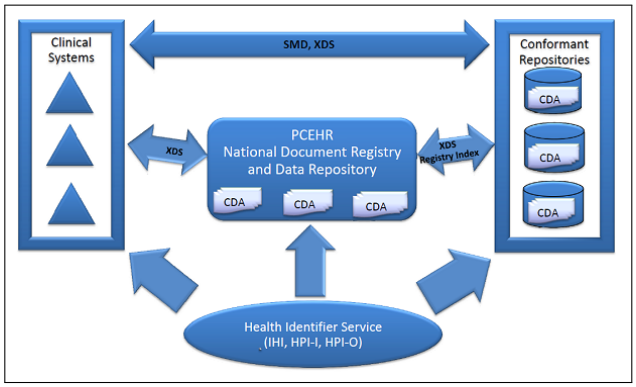

Figure 2: Diagrammatic Representation of the PCEHR

The PCEHR architecture consists of the following services and standards:

- Health Identifier (HI) Service – service specified by NeHTA and implemented by Medicare
- Secure Message Delivery (SMD) – Standards Australia Technical Specification
- Clinical Document Architecture (CDA) – Health Level 7 (HL7) Standard
- Cross Enterprise Document Sharing (XDS) – Integrating the Health Enterprise (IHE) Profile
- ISO 27790 Health informatics: Document registry framework - International Organization for Standardization
- National Authentication Service for Health (NASH) – service specified by NeHTA, implemented by IBM under a government contract.

The proven combination of CDA and XDS.b as a secure clinical document exchange facility, should provide core capability that will reward future investment in functionality and content. This is an ambitious, diverse and integrated architecture whose local components are as yet unproven, however they are based on proven widely deployed international standards and profiles. Significant changes have been made for the Australian implementation, some of which have not yet been fully disclosed and hence it is difficult to evaluate the total impact on functionality, performance and security. It is clear that the variance is sufficient to place a barrier in the path of participation by international vendors as well as potentially limiting export opportunities for local implementers.

Of concern is that in any electronic records system it is the control of all information, but particularly sensitive and patient confidential healthcare data that needs protection. The manner that this is dealt with from a security perspective is through established security policy. This requires that all participants in the information sharing domain in question must have methods of informing each other of their respective policy and ensure they are consistent [19]. This extends further than just trusted end-to-end communication. Privacy of information has been, and is, a major issue for all countries in developing shared healthcare data systems [20]. Whilst there exists a National Ehealth Security and Access Framework (NESAF) [21] intended to provide an overall architectural solution for security, it is the application of this aspect that is currently unclear in Australia's deployment. The NESAF itself is based primarily and extensively on ISO standards and whilst still under development themselves, refers to the HL7 PASS and SAIF frameworks [22].

A recent article by NeHTA's Chief Clinical Lead and other well respected co-authors suggest that there may be critical unmitigated risks with the current implementation [23]. The need for bespoke tool kits for development and conformance testing is a flow-on from the variations to international standards and represent a further risk in terms of possible uncaught implementation errors and ongoing maintenance costs. There will be a necessary trade off between complexity of regulations, conformance and compliance requirements, and an implementation barrier and cost that may prove difficult to manage. This is likely to lead to delays in implementation as has been evidenced already by the Health Identifiers Service. Delays of up to two years for significant uptake have been forecast in DoHA and NeHTA presentations. These important factors result in a number of challenges for those who are to engage with the implementation and use of the national PCEHR system in a commercially sustainable environment.

3 Community and Stakeholder Challenges

The situation described above has led to a number of tensions between government and industry. Numerous personnel changes and strong political drivers pushing for short time frames have detrimentally impacted collaboration with the stakeholders and made quality development challenging. It has seen short term planning, decision making and frequently changing goal posts, which create frustration and uncertainty about what can and will be delivered. Indeed the scope of what will be deliverable on July 1st, 2012 has been constrained considerably from its original specification over the period from April 2012.

From a software industry perspective the tensions are compounded by the issues resulting from the government's inflexibility on time frames and initial scope creep followed by a rapid reduction in scope in the months prior

to launch. There is considerable pressure to realise return on investment as despite being a national initiative, the majority of the software industry is not being funded to implement the attached systems. Given the changes, delay in some specifications and lack of budget for long term development of specifications, the scope has now been so constrained and it may prove difficult to make a sustainable business case for implementation for many vendors in the short or medium term.

One significant issue that has arisen is that some standards have been varied during implementation. For instance, the HL7 CDA standards have been extended, the impact of which is that the standard tools and testing methodologies do not work with the NeHTA versions. The IHE XDS payload and XML packaging have been altered from the international profile. The security in the PCEHR has not been disclosed other than in the broadest terms. There are issues of late modifications to both the PCEHR electronic (B2B) interface and content specifications which will ensure that implementation will take time once the specifications are available, correct and stable. Lastly, the delivery of associated but fundamental services, for instance the NASH, has been delayed, and now is only due for delivery sometime after the 1 July PCEHR launch date, necessitating the adoption of interim security arrangements which have recieved little external scutiny. It is very difficult to retrofit security and there is no information provided on the extensions to standard PKI certificates that will be employed. There are concerns that appropriate Health Identifiers Service functionality may not be in place prior to PCEHR launch. For instance, the ability to assign patient individual health identifiers (IHIs) to neonates in a timely manner.

In regard to the clinical community, there are many issues that have yet to be fully addressed associated with clinical workflows and sustainability. Firstly, the incentives to use the PCEHR are not clearly defined from the clinician perspective though there has been some clarification about use of claimable service fees (called item numbers in the Australian context). Secondly, there are risks to the information being shared and available in many places but uncertainty that it is complete. The quality of the patient summaries may be variable since patients can nominate any provider to submit this information at any time. This may not be their usual practitioner or one that has the majority of relevant information for the patient. This is complicated by the potential commercial incentives for a variety of providers to undertake this activity. The currency of data and any implied obligations on the practitioner who submitted it to the PCEHR have not been widely discussed. The willingness or ability of clinicians to construct appropriate summaries for upload has been assumed rather than tested in any large scale deployment. This was not possible in the test implementation (Wave 2) sites as they did not connect to the PCEHR and employed a completely different interface technology to separate repositories.

From the public's viewpoint there has been little published testing of the impact of the PCEHR and in particular the consumer entered information including what impact this may have on the patient/consumer themselves. There are two parts to the patient entered information - a private and a clinical section. The consumer has control of this information and to whom it is visible. What if inappropriate comments about their treating clinicians or GP are entered? For example a disgruntled patient posted information of a detrimental nature about their doctor. Whether there are adequate safeguards is unclear at present.

Secondly, the decision making ability of the consumer in regards to the control of their information also raises concerns. How are the general public (not medically trained or aware) to decide what clinical information, which they may or may not understand, is relevant or meaningful. Would a patient understand that an x-ray report of pneumocystis pneumonia would be primary evidence for most medical practitioners that the patient has HIV? It is clear that patients will have to understand complex medical data in order to put in place effective and desired access control. For some sections of the community this may cause anxiety in the decision making and distrust influencing the decision to conceal or not conceal certain information. Patients making these choices may not completely understand the implications of hiding data on their future treatment.

4 Conclusions

The development of a service oriented architectural solution on a national basis is ambitious yet necessary. The successful deployment of a national health records system, regardless of any technological issues, is dependent ultimately on the user acceptance and use. Putting the legal, workflow and security barriers aside, the standardisation of healthcare information (yes more standards) is a key element to its adoption.

The initial facilities will be basic and any uptake will be dependent on funding to extend and prove the system. This is likely to take a significant time and in the current political environment may not even be possible. Of greater concern is the lack of a live test environment, similar to a live deployment but with populated dummy data with which to test the security, access and performance. Any large implementation that has a high reliance on and integration of security services, as the Australian national ehealth system undoubtedly has, should have a coordinated and defined security test plan. To date no such plan has been released or reported on. In fact the security deployment has been kept confidential. In a system that reflects a security based services oriented architecture, the necessity to test the individual components and the integrated end-to-end system is vital. Whilst the underpinning of the system and its reliance on standards will provide some assurance, what is untested is the variation from these established international standards. Post

1 July, 2012 will provide some of these answers.

References

[1] Carro SA, Scharcanski J. A framework for medical visual information exchange on the web. Comput Biol Med. 2006;36.

[2] Pharow P, Blobel B. Security Infrastructure Services for Electronic Archives and Electronic Health Records. In: Bos L, Laxminarayan S, Marsh A, editors. Studies in Health Technology and Informatics: Medical and Care Compunetics 1: IOS Press; 2004. p. 434 - 40.

[3] Commonwealth of Australia. Improving Primary Health Care for All Australians. Commonwealth of Australia; 2011.

[4] Department of Health and Aging. National Health Reform: eHealth. Australian Government; 2012 (cited 2012 23 June); Available from: http://www.yourhealth.gov.au/-internet/yourhealth/publishing.nsf/Content/theme-ehealth

[5] Council of Australian Governments. National Health Reform Agreement. In: Aging DoHa, editor.: Australian Government; 2011. p. 70.

[6] NEHTA. eHealth: About the PCEHR system. National eHealth Transition Authority; n.d. (cited 2012 23 June); Available from: http://www.ehealthinfo.gov.au/personally-controlled-electronic-health-records/about-the-pcehr-system.

[7] Australian Government. Concept of Operations: Relating to the introduction of a Personally Controlled Electronic Health Record System: Commonwealth of Australia; 2011. Available from: http://www.yourhealth.gov.au/internet/yourhealth/-publishing.nsf/Content/PCEHRS-Intro-toc

[8] Health Information Standards Organisation. Why standards? n.d. (cited 2006 09 March); Available from: http://www.hiso.govt.nz/whystandards.htm

[9] Ahmad S. Why Should Companies Support Standards Development? Nuclear Standards News (serial on the Internet). 2002 (cited 2012 23 June); 33(6): Available from: http://www.new.ans.org/standards/resources/articles/nsn-comsupport.php (last access on December 30 2012)

[10] Williams PAH. The role of standards in medical information security: An opportunity for improvement. In: Arabnia HR, Aissi S, editors. The 2006 World Congress in Computer Science, Computer Engineering, and Applied Computing - SAM'06 - The 2006 International Conference on Security & Management. Monte Carlo Resort, Las Vegas, Nevada, USA (June 26-29, 2006) 2006. p. 415-20.

[11] International Organisations for Standards. Discover ISO: Who standards benefit. ISO; 2011 (cited 2012 23 June); Available from: http://www.iso.org/iso/about/discovers-iso_who-standards-benefits.htm

[12] Raghupathi W, Kesh S. Interoperable Electronic Health Records Design: Towards a Service-Oriented Architecture. E - Service Journal. 2007;5(3):39-57.

[13] Welke R, Hirschheim R, Schwarz A. Service-Oriented Architecture Maturity. Computer. 2011;44(2):61-7.

[14] Holt J. Standards development. The Computer Bulletin. 2004 November 1, 2004;46(6):28.

[15] Hammond WEP, Jaffe C, Kush RDP. Healthcare Standards Development: The Value of Nurturing Collaboration. Journal of AHIMA. 2009;80(7):44-52.

[16] IHE. IHE IT Infrastructure. IHE International; 2011 (cited 2012 01 May); Available from: http://www.ihe.net/IT_Infra/committees/ (last access on December 30 2012)

[17] de Lusignan S, Krause P. Liberating the NHS: an information revolution - -think beyond the electronic patient record, think service oriented archtecture! Informatics in Primary Care. 2010;18:147-8.

[18] Channabasavaia K, Tuggle E, Holley K. Migrating to a services orientated architecture. IBM; n.d. (cited 2012 1 May); Available from: www.ibm.com/developerworks/library/ws-migratesoa/#figure1 (last access on December 30 2012)

[19] Katehakis DG, Sfakianakis SG, Kavlentakis G, Anthoulakis DN, Tsiknakis M. Delivering a Lifelong Integrated Electronic Health Record Based on a Service Oriented Architecture. Information Technology in Biomedicine, IEEE Transactions on. 2007;11(6):639-50.

[20] Gupta V, Murtaza MB. Approaches To Electronic Health Record Implementation. The Review of Business Information Systems. 2009;13(4):21-8.

[21] NEHTA. NESAF R3.1 Executive Summary2012 (cited 2012 23 June); (Version 3.1): Available from: http://www.nehta.gov.au/connecting-australia/ehealth-information-security

[22] NEHTA. NESAF Release 3.1: Standards Mapping (S1410)2012 (cited 2012 23 June); (Version 3.1): Available from: http://www.nehta.gov.au/connecting-australia/ehealth-information-security

[23] Coiera EW, Kidd MR, Haikerwal MC. A call for national e-health clinical safety governance. Medical Journal of Australia. 2012;196(7):430-1.

