1-1-2012

Building patient trust in electronic health records

Helen Cripps

Craig Standing
Edith Cowan University

Originally published in the Proceedings of the 1st Australian eHealth Informatics and Security Conference, held on the 3rd-5th December, 2012 at Novotel Langley Hotel, Perth, Western Australia

BUILDING PATIENT TRUST IN ELECTRONIC HEALTH RECORDS

Helen Cripps[1], Craig Standing[2]
[1,2]The Centre for Innovative Practice, Edith Cowan University, Australia
[1]h.cripps@ecu.edu.au, [2]c.standing@ecu.edu.au

Abstract
While electronic medical records have the potential to vastly improve a patient's health care, their introduction also raises new and complex security and privacy issues. The challenge of preserving what patients' believe as their privacy in the context of the introduction of the Personally Controlled Electronic Health Record (PCEHR), into the multi-layered and decentralised Australian health system is discussed. Based on a number of European case studies the paper outlines the institutional measures for privacy and security that have been put in place, and compares them with the current status in Australia. The implementation of the PCEHR has not been as straight forward, holistic or as uniform as in the European countries' studied. This has meant that issues around personal privacy and security have not been addressed in an effective and functional manner. Surprisingly, the researchers found that the patient is absent in the PCEHR privacy and security discussion; and their perceptions of, and requirements for privacy and secure management of their medical information is absent. The concept of personal privacy and security has yet to be fully explored from the patient's perspective, despite it being a ***Personally*** *Controlled Health Record.*

Keywords
Electronic health records, privacy, security, patients

INTRODUCTION

The application of information technology to medicine is not new, with General Practitioners (GPs) adopting electronic medical records as early as the mid-1980s (Mahncke & Williams, 2006). Similarly, the keeping of electronic records within the business and the management of individual's personal finances is well established. Online banking has been available since the late 1980s and took off in the mid 1990's with the advent of the web-based banking. Data is accessed electronically via pin numbers, cards and web pages ("Canstar: online-banking history," 2012). Health information could be considered to be far more sensitive than other personal data, but as retail outlets and retailer loyalty programs have demonstrated for years, that people are willing to disclose some personal information in return for perceived tangible benefits. The concept of disclosure in return for better treatment could be applied to health data as well ('Health IT Exchange: Building patient trust in EHRs can't be about security," 2010). With the benefits of shared and accessible health information there is always a price in relation privacy and security (Rynning, 2007).

The disclosure of personal medical information highlights the issues of trust and its role in relation to the privacy and security of electronic health records (EHRs) that are far more complex because there are multiple parties involved. A simple way to view trust is as a willingness to take risk (the risk in this case comes from one party making themselves vulnerable to the actions of another based on the expectation that the other party will behave in the way desired by the trusting party). It is suggested that context is also essential, where trust is a three-part concept, involving a truster, a trustee, and a purpose or scope to which the relationship applies (Baier, 1986; Hardin, 1993). In the case of EHRs, the patient makes themselves vulnerable to the clinicians by disclosing personal medical information trusting that it will be managed in an appropriate manner. The context of trust has become more complex due to the introduction of digital information and the potential interoperability and of records (Alhaqbani & Fidge, 2007).

If the technical security issues are not addressed in a way that patients understand and accept them, then it is possible the patient will lose confidence and trust in the EHR system. This lack of trust may lead to patients not providing information in an attempt to preserve their privacy, thus affecting the integrity of the stored data and potentially leading to life-threatening situations such as inappropriate medication (Alhaqbani and Fidge, 2007). It is suggested by Jacques (2011), that in order for patients to have a greater level of control over their privacy they should be allowed to opt into the EHR system or at least flag and restrict sensitive information.

Coles-Kemp and Kani-Zabihi (2011) suggest that an individual's interaction with any online information system is multilayered in nature; there is the physical, informational, personal and communal layers. The physical and information layers usually provide privacy protection. Their study highlighted the divide between the person and

the institutional system with which they interact. Previously interactions with institutions have been conducted on a face to face basis, however with the advent of technology there has been a shift to the use of a digital interface instead of a personal one (Coles-Kemp & Kani-Zabihi, 2011).

With the introduction of EHRs, an additional set of players and factors have entered the equation such as electronic security protocols on EHR systems, privacy legislation, government protocols and electronic interchange of patient data. There is a disconnect between institutional systems for the privacy and security of EHRs and the patient's perceived personal security and privacy of information stored on EHRs. The lack of integration between institutional and personal requirements for privacy and security is illustrated in figure 1 below.

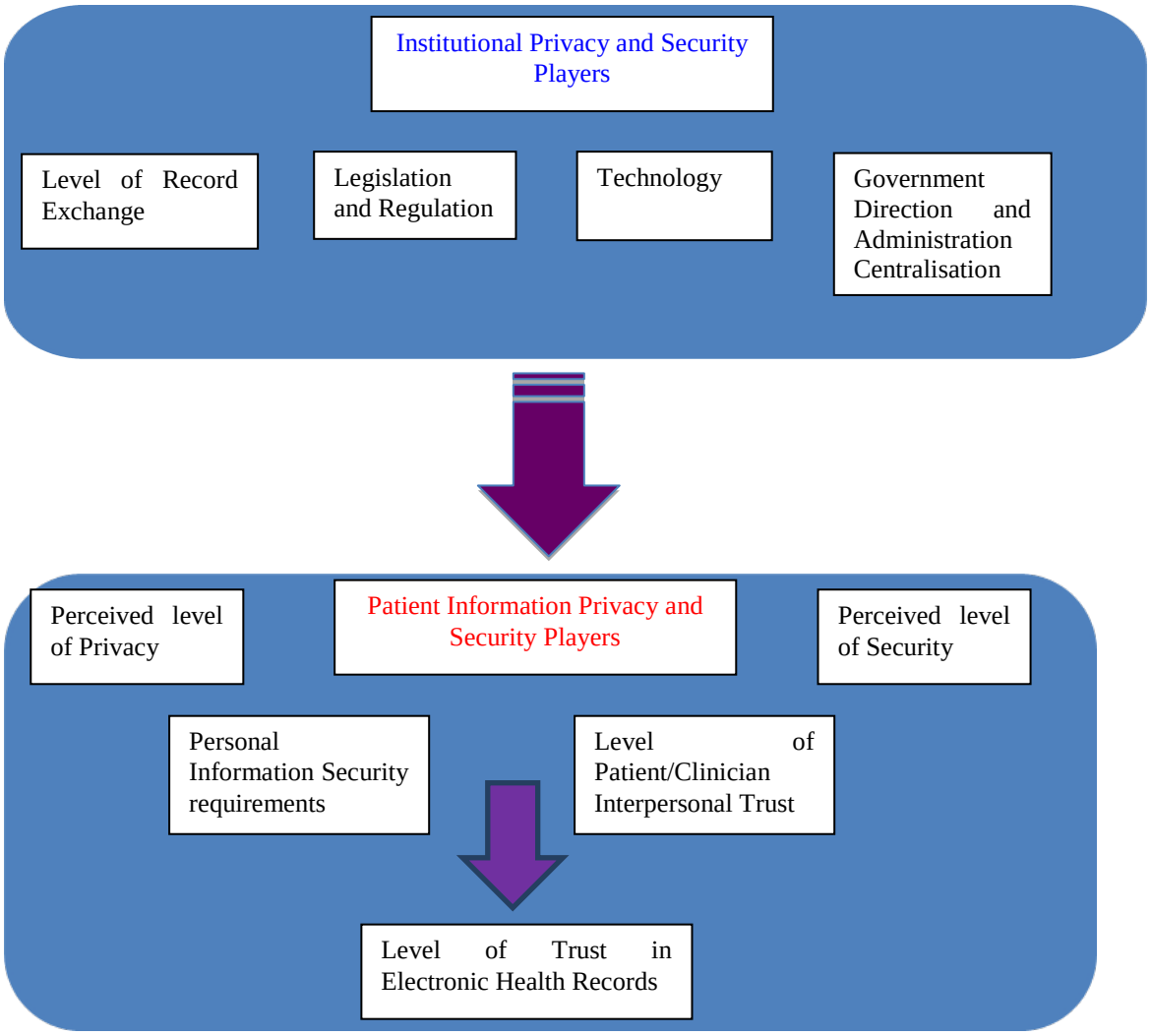

Figure 1 - Institutional and personal requirements for privacy

Privacy and Security Issues in Electronic Health Record Systems

While much of the recent attention on EHRs has been on the establishment and integration of computer systems, little attention has been paid to privacy and security in the health context. From a technical standpoint patients have voiced their concerns about their medical records being stored and used in electronic form citing issues including loss, theft, and misuse of what they consider private and personal information. It has been suggested that the emphasis on privacy and security in EHR systems as a requirement for building consumer trust in these systems. The reliance on institutional security controls, underestimates the importance of the provider-to-patient relationship in the formation of trust. According to a review by Tejero and de la Torre (2011) the weaknesses if the EHRs they reviewed included a lack of interoperability, a supporting legal framework yet to be established,

sensitive information that is not protected, the reliance on the physicians for EHR adoption and the risk of data theft and phishing.

Moving from a paper file to an electronic record means that information is no longer physical but digital and therefore can more easily be moved. Once all a patient's information was kept in a paper base file in a clinic or hospital, held in what was presumed a secure location. It could be suggested that the patient's trust was placed in the institution or practice in which the paper file was held. Now given the complexity and portability of current electronic systems, it is unrealistic to think patients would be able to learn or understand the technical information about EHR systems, let alone have the level of understanding that the providers or hospitals or insurance companies use ('Health IT Exchange: Building patient trust in EHRs can't be about security," 2010).

Without a detailed understanding of the system it is unlikely that patients would be able to make an independent determination as to whether the privacy and security measures afforded by such a system are sufficient to make them confident that their personal health data is protected. Instead, most people will rely on their doctors or other providers (the actual users of the EHR systems), and their relative comfort level with digitising their health records will likely be strongly correlated to the level of trust they put in their providers (Health IT Exchange: Building patient trust in EHRs can't be about security, 2010).

Measures to Address Privacy and Security Issues in the Australian Context

Showell (2011) contends that Australians will have had little prior exposure to policy issues of privacy, consent and secondary use, and may feel that they have not been adequately consulted. Mistrust, scepticism and caution may lead to resistance to the introduction and uptake of the EHR system, and result in a reiteration of adverse views which may already have been addressed effectively. To achieve a completely operational EHR platform, security and privacy problems have to be resolved, due to the importance of the data included within these records. But given all the different methods to address security and privacy, they still remain in most cases as an open issue (Showell, 2011).

As early as 2006 the Australian Privacy Foundation, flagged the privacy risks inherent in any system of EHRs to include poor security where patients and unauthorised people may be able to access the patient's records leading to inappropriate access to records and theft of personal data. For example, the unauthorised exchange of information with other health care providers such as pharmaceutical companies; and the use of a consolidated health record by a patient's employer or insurance company for discriminative employment practices. Those responsible for designing EHR systems should ensure that these risks be minimised as much as possible, by using the best technology, legal safeguards, policies, procedures, and training. Specifically, patient education was not addressed in these recommendations (Australian Privacy Foundation, 2006).

The changes to health care system and the move to personally controlled health records has reframed patients as 'consumers', with an assumption that they have a consumer's right to select and choose in the health marketplace and are participants in the development of their e-health record. There is little evidence of direct citizen involvement in the discourse about the EHR, or about health identifiers. Neither is there much visible evidence of widespread public discussion or debate about the policy issues, or evidence that the general public has any working knowledge of the proposed EHR system, and how it will operate in practice (Showell, 2011).

The recommendations from the Office of the Privacy Commissioner (OPC) in 2006 addressed patients' privacy concerns and suggested the following measures; an opt-in consent model, a multi-layered approach to consent, consumer control over access to their health information, capacity to mask sensitive information, elimination of regulatory complexity and uncertainty, and some control over secondary uses of health information. At this time, the OPC warned against forming a view of the 'normal consumer'. An individuals' perception of how their health information is handled is personal and subjective, and systems need the flexibility to accommodate people holding different views about how much of their own health information should be confidential (Consumer's Health Forum, 2006).

Yet six years after original concerns were raised around privacy and security, it would seem little has been done. According to recent media reports by the Australian Broadcasting Cooperation and, associations such as the Australian Medical Association (AMA), the privacy issues mentioned above are yet to be tackled. Medical experts have highlighted some of the risks as Australia moves into a system of EHRs. Doctors are warning it is vital to ensure personal records do not become compromised, as the range of electronic devices available for access grows. The system needed to be secure whether used from a personal computer, tablet or smart phone and there was concern that unauthorised people might access someone else's notes, if devices were left open or accessible.

Launch of the Personally Controlled Electronic Health Record (PCEHR) System in Australia

Australia has a two-tiered government system (state and federal) that is responsible for the delivery of health services. An additional layer of complexity is the presence of a large private health sector which is not directly under the government's control. In Australia, individual general practices have implemented EHR systems, with no patient input. The implementation of such systems in hospitals and general practices has been very piece meal with no uniformity or consistency as adoption was driven by information technology (IT) vendors. The Australian government considered that the introduction of personally controlled electronic health records would enable people to take a more active role in managing their health and making informed decisions (National Health and Hospitals Reform Commission, 2009). This belief led the government to establish the PCEHR launched on 1 July 2012.

Australians can now choose to register for their own personally controlled eHealth record. An eHealth record is an electronic summary of an individual's key health information. Initially an eHealth record will contain basic information. As the system develops, healthcare providers will be able to add more information like treatments, medications and allergies. Individuals can control their own eHealth record, by choosing to restrict which health care provider organisations can access it and what information is included. Patients can volunteer to join the system (via the department's website), which stores all their health information, including test results and prescriptions, in a national database. It is the first time patients will be able to access their medical details.

Since the launch of the PCEHR, only 5,029 people have joined the federal government's controversial $466 million eHealth system. Figures obtained from the Department of Health and Ageing has shown each individual to take up the PCEHR has so far cost the government $92,662 (Molloy, 2012). The slow uptake had been predicted in May, and confirmed soon after the online database commenced. A month later, glitches were revealed with the system.

Implementation of Electronic Health Records in Europe- Selected cases

The implementation of EHRs in Europe has a significantly longer history than in Australia. Generally, the European countries that have had communist or socialist governments have a more centralised health system with tighter government controls. This has made the link between legislation, clinicians and IT vendors more effective in delivering a secure and trusted EHR system. Case studies were conducted during 2010-2011 to investigate the process of implementation of EHRs in three selected European countries, Finland, Norway and Slovenia. The interviews were conducted with the clinicians; government and IT vendors. The findings collected have been summarised around the themes of privacy and security.

The Characteristics of the European System

The research found that in each case a considerable legislative framework had been put in place prior to the implementation of an EHR system, to support information security and patient privacy. The legislation included penalties for non-compliance and privacy breaches. Due to the centralised government system and health infrastructure, uniform processes were established at all levels of the health system. As a result, IT system specifications have been developed and built into the IT to address privacy and security issues. In fact, one of the respondents stated "The data is actually more secure than when we had medical data on paper, as there was no tracking when and who accessed the data. Now we have electronic records, any access to the data can be tracked" (Medical Administrator, Slovenia). In Slovenia, the Information Commissioner reviews the security of personal data held by medical providers on the EHRs. In fact, the respondents' organisation had been reviewed by the Information Commissioner three weeks prior to the interview and had received recommendations on areas of security upgrade.

The health agency known as Kela in Finland, has been running some form of electronic demographic database for the past 50 years. As part of the development of a single national health database, rules have been developed as to who can access what part of the data. The management of medical records is based on each document being considered as to what should be put on the common record. Guidelines as to who can have access to what information are held on each file, and which medical professionals can see what.

Security has not proved an issue in Norway, as there have been no incidences of identity theft, and criminals generally have no interest in what is stored on a patient's EHRs. Patients cannot access their records at this point in time, except in the Doctor's office or via a bedside terminal. According to one interviewee, the records are written for the Doctor's requirements, not for the patients' needs and hence could be misinterpreted if the patient was to view the record without a practitioner being present.

The downside of the highly centralised health systems in Europe is the direct intervention by ministers and law makers. According to one respondent in Finland, "one of the risks is Parliamentary involvement and influence in the process, is that laws can be changed to enable people to be profiled through the system." Although

significant institutional safe guards have been put in place in the health systems examined, the major source of risk is not electronic but human. One of the risks identified is poor practices around the input of management and data by clinicians, as exemplified by the following comment "If the Doctors do not like it then they do not use it and the system will not work. A poor interface will not be used and this will leave both Doctors and patients without information." The more people that access the system, the higher the security risk and the demands from a wide range of system users often makes it difficult to develop a standard format for the EHR. Despite electronic records being part of the medical system for over 20 years, there is still a human resource issue. A health administrator in Slovenia stated that "the major resource issue is the lack of people who have skill and experience in health informatics as under the current scheme people are not a priority". Without skilled people the EHR systems will not function.

From the data collected, the European system had the advantage of a more centralised implementation process for EHRs. The advantages of this are a consistent legislative framework and practices around patient information privacy and security, relatively standardised IT systems and information management practices. Despite this uniformity, none of the three countries investigated has yet established a national interoperable EHRs database.

Current Status in Australia

Laws relating to health information privacy at the state and federal government level in Australia

In order to provide a legislative framework for the management of patient information, the Australian government is proposing to introduce the 'Personally Controlled Electronic Health Records Act 2012' (PCEHR Act), establishing the personally controlled electronic health (eHealth) record system and provides for its regulatory framework. Under the proposed Act will give the Information Commissioner (the Commissioner) the power to investigate alleged contraventions of the Act and pursue enforcement mechanisms that are appropriate in the circumstances of the case (Office of the Australian Information Commissioner, [OAIC], 2012).

The AMA in its submission to the Department of Health and Ageing expressed the need to ensure that only people who have a genuine need and are authorised to do so are entitled to access a person's PCEHR. The legislation should also set out the framework under which the PCEHR system operator will function and the requirements on the repository operators. The regulatory burden of the PCEHR on medical practitioners should be kept to an absolute minimum (OAIC, 2011). The Australian government has allowed doctors to be compensated for the extra work involved in supporting the system, in recognition of the additional time required to maintain EHRs (Australian Medicine, 2012).

Another parallel issue raised with the advent of electronic records is the level of patient access. Once paper health records were held by the clinician and rarely viewed by the patient. Now with PCEHRs, issues have been raised by about the level of patient access and understanding. From the case studies carried out in Europe clinicians expressed concerns around the complexity of data being stored in the EHRs and rarely are patients allowed to access their records without a clinician present to interpret the data. It not just the relationship between the EHR system in place and the patient, the clinician plays a mediating role between the system and the patient ('Health IT Exchange: Building patient trust in EHRs can't be about security," 2010).

CONCLUSION

A common feature across the implementation of EHRs is the disregard of the patient's needs and understanding of privacy and security of their personal medical details. In Australia, legal and technical infrastructure is being put into place, as in the European countries examined. A patient's understanding of EHRs has yet to be addressed, as highlighted in a recent study in the United Kingdom where it was found that over 50% of patients would withhold information to their health care provider due to privacy concerns. So no matter how stringent the privacy and security measures, the accuracy of the data and its eventual usefulness are based on the patient's trust in the EHR (FairWarning, 2011).

For the PCEHR to be successfully implemented there needs to be education and promotion of EHRs of their intended and permitted uses and benefits, and also the ways in which personal health data is protected against loss, theft, misuse, and unauthorised disclosure. The best way to deliver these messages is to leverage the (hopefully) trusting relationship that already exists between patients and providers, since from the patient perspective, their doctors are much more likely to take on patient interests as their own than EHR software vendors, insurance companies, or even government health agencies ('Health IT Exchange: Building patient trust in EHRs can't be about security," 2010).

The point is not to down-grade the importance of having strong privacy and security protections for health data stored in EHR systems, but instead to reiterate that patient trust (or lack thereof) in health IT cannot be provided through technical means alone. Patients may not know how their medical records are stored (paper files,

computer, or some combination) or the physical, technical, or administrative measures in place to secure them. With the prospect of easier and more frequent sharing of health data enabled by EHR systems, patients may have less control over how their records are being handled. Well informed patients who trust in the privacy and security of their health records would seem to be a prerequisite for the effective implementation of EHRs. Without this the benefits to themselves, their health care providers, and the health care system will not be realised.

The PCEHR is only beneficial as the patient information it contains. The EHR will be compromised if the patient chooses to withhold vital information due to privacy and security concerns. Thus lowering the clinicians trust when the record is viewed in a different health setting such as an emergency department. While the Australian federal government has sought to tackle the technological and now legal issues surrounding privacy and security, the PCEHR could fail if its target audience; the patient fails to opt in.

Considering the relatively low uptake of the PCEHR to date, it would suggest that there is a low level of acceptance of and trust in EHRs. Further research could be conducted around patients' privacy and security needs and how best these can be met in the implementation of the PCEHR. Unlike Europe with its centralised implementation, consistent legislative and administrative framework and history of national EHRs, Australia has many more obstacles to overcome for the successful implementation of EHRs.

REFERENCES

Alhaqbani, B.S. and Fidge, C.J. (2007). *Access Control Requirements for Processing Electronic Health Records*. Business Process Management Workshops, Queensland University of Technology, Brisbane, 4928, pp. 371-382.

Australian Medicine Online. (2012). *Doctors win recognition for PCEHR work*. Australian Medicine - 3 September 2012. Retrieved from http://ausmed.ama.com.au/doctors-win-recognition-pcehr-work

Australian Privacy Foundation, 2006- *Campaigns Health E Link NSW. NSW trial of EHRs*. Retrieved from www.privacy.org.au/Papers/indexPolicies.html

Baier, A. (1986). Trust and antitrust. *Ethics, 96* (2), 231-260.

Canstar. (2012). History of Online Internet Banking in Australia. Retrieved from http://www.canstar.com.au/online-banking/history/

Coles-Kemp, L. & Kani-Zabihi, E. (2011). *Practice Makes Perfect. Motivating confident privacy protection practices*. The Institute of Electrical and Electronics Engineers (IEEE) International Conference on Privacy, Security, Risk, and Trust, and the IEEE International Conference on Social Computing. Retrieved from http://www.iisocialcom.org/conference/passat2012/PASSATProceedings/data/4578a866.pdf

Consumers' Health Forum of Australia: E-health National Information Workshop. Canberra 29-30 May 2006. Retrieved from http://www.chf.org.au/pdfs/rep/rep-413-e-health-workshop.pdf

FairWarning. (2011). UK: How Privacy Considerations Drive Patient Decisions and Impact Patient Care Outcomes. New London Consulting. Retrieved from http://www.ehealthnews.eu/images/stories/pdf/2011-WHITEPAPER-UK-PATIENT-SURVEY.pdf

Hardin, R. (1993). The street-level epistemology of trust. *Politics and Society, 21*(4), 505-529.

Health IT Exchange. (2010). *Building patient trust in EHRs can't be about security controls.* Retrieved from http://www.searchhealthit.techtarget.com › ... › IT Blogs › HIT Security and Privacy. Posted by: SteveGonhit 19 June 2010.

Jacques, L.B. (2011). Electronic health records and respect for patient privacy: A prescription for compatibility. *Vanderbilt Journal of Entertainment and Technology Law, 13*(2), 441.

Mahncke, R. & Williams, P. A. H. (2006). Secure transmission of shared electronic health records: A review. In C. Valli and A. Woodward (Eds.), *Proceedings of the 4th Australian Information Security Management Conference*, 184-195, School of Computer and Information Science, Edith Cowan University, Perth, WA.

Molloy, F. (2012). *E-health records' security at risk.* Retrieved from http://www.theage.com.au › IT Pro › Government IT.

National Health and Hospitals Reform Commission. (2009). A healthier future for all Australians - Final Report of the National Health and Hospitals Reform Commission – June 2009. Retrieved from http://www.health.gov.au/internet/nhhrc/publishing.nsf/Content/nhhrc-report

Rynning, E. (2007). Public trust and privacy in shared electronic health record. *European Journal of Health Law, 14*(2), 105.

Showel1, C.M. (2011). Citizens, patients and policy: a challenge for Australia's national electronic health record. *Health Information Management Journal, 40* (2), 39-43.

The Office of the Australian Information Commissioner (OAIC). (2012). *eHealth record system: The Office of the Australian Information Commissioner Enforcement Guidelines*. Retrieved from http://www.oaic.gov.au/news/consultations.html#enforcement_guideline

The Office of the Australian Information Commissioner (OAIC). (2011). *Personally Controlled Electronic Health Record (PCEHR) System: Legislation Issues Paper*. Submission to the Department of Health and Ageing. Retrieved from http://www.oaic.gov.au/publications/submissions/2011_08_submission_personally_controlled_ehealth.pdf