6-2013

Perceptions of Security, Privacy and Confidentiality in the Context of Electronic Health: The Gap between Institutions and Patients

Helen Cripps
Edith Cowan University, Australia, h.cripps@ecu.edu.au

Craig Standing
Edith Cowan University, Australia, c.standing@ecu.edu.au

26th Bled eConference

eInnovations:
Challenges and Impacts for Individuals, Organizations and Society

June 9, 2013 – June 13, 2013; Bled, Slovenia

Perceptions of Security, Privacy and Confidentiality in the Context of Electronic Health: The Gap between Institutions and Patients

Helen Cripps
Edith Cowan University, Australia
h.cripps@ecu.edu.au

Craig Standing
Edith Cowan University, Australia
c.standing@ecu.edu.au

Abstract

While electronic health records have the potential to vastly improve a patient's health care, their introduction also raises new and complex issues around security and privacy. There are significant challenges in preserving what patients' believe to be their privacy and confidentiality, in the context of the accessibility and interoperability of electronic records. Based on a number of expert interviews the paper outlines the institutional measures for security that have been put in place, and highlights the lack of discussion around individual patient privacy requirements. Whilst institutional measures such as legislation, technology and standardised systems have been established, the interpersonal nature of privacy and confidentiality from the patient's perspective has yet to be addressed.

Keywords: Electronic health records, privacy, security, patients

1 Introduction

The application of information technology in medicine is not new, with General Practitioners (GPs) in Australia adopting electronic medical records as early as the mid-1980s (Mahncke and Williams, 2006; Jha et al., 2008). Similarly, electronic record keeping for the management of individual's personal finances has been 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. Personal financial data is now accessed electronically via pin numbers, cards, webpages and mobile devices ("Canstar: online-banking history", 2012). The proliferation of technology including, wireless networks and mobile devices, will created even greater challenges for the securing of data, in both the business and health settings (Istepanaian and Zhang, 2012). On the human side of the privacy equation are the changing perceptions of personal privacy online due to advent of social networking sites such as Facebook (MacDermott and Smith, 2103).

2 Privacy and IT System Security

The introduction of Electronic Health Records (EHRs) into the medical system has created an additional set of factors surrounding the relationship between the patient and the clinician. These additional players include; medical administrators, IT system vendors, electronic security protocols on EHR systems, privacy legislation, government policy and electronic interchange of patient data between institutions. The introduction of EHRs also poses additional ethical issues for clinicians around their interactions with patients in the areas of online practice, the gaining of informed consent, privacy, security and confidentiality. Although these issues are present in other areas of online administration, such as e-business and e-government, the life and death nature of health care magnifies these issues (Wickramasinghe, et al., 2005).

A review in 2011, of e-health adoption in Europe found that privacy, confidentiality, liability and data protection all need to be addressed for the successful implementation of EHRs. A specifically short fall was the lack of coherent laws designed to address all aspects of privacy in e-health (Stroetmann et al., 2011). In the context of EHRs there needs to be a balance between the technical requirements and specifications for the storage of health information, and the privacy and security polices required to protect the data. According to Bauer (2009), the implementation of EHRs should not compromise the basic human right for privacy, however there seems to be a disconnect between institutional systems for the privacy and security of EHRs, and the individual patient's perceived personal requirements around the security, privacy and confidentiality of their information stored on EHRs.

To date, the discussion and research around the management of EHRs has focused on institutional measures such as privacy laws, IT security protocols and administrative measures as a means of creating privacy around patient data. Based on a review of the literature and key informant interviews, the authors suggest that security, privacy and confidentiality, while interlinked, are very different concepts when viewed from a patient's perspective. The institutional means employed to secure patients' EHRs do not necessarily ensure the level of privacy and confidentiality required by the individual patient. The level of privacy and confidentiality required will vary from patient to patient and cannot be institutionalised or uniformly addressed in the same manner as EHR security personal privacy requirements in the digital realm are far from standardised or codified as a standard or 'normal' patient does not exist (Consumers' Health Forum of Australia, 2006). The patients trust in their EHR is a combination of the institutional measure and the patient's personal privacy needs.

3 Privacy and Security Issues in Electronic Health Record Systems

Much of the recent attention on EHRs has been on the establishment and integration of EHRs with less attention on privacy and security issues. Additionally, ongoing turbulence in the e-health systems market place has stymied, attempts to standardise EHRs to create interoperability (Anderson, 2007). According to a review by Tejero and de la Torre (2011), the weaknesses of the EHRs they reviewed included a lack of interoperability, a supporting

legal framework, the storage of unprotected sensitive information, the reliance on the clinicians for EHR adoption, and the risk of data theft and phishing.

Legislation and technology have been the main strategies used to maintain the security of EHRs. Bauer (2009) makes a differentiation between these codifiable strategies designed to maintain privacy and the "'human system' such as the relationship between the patient and the clinician that is not subject to codification in the same way that data on electronic records is codified. Additional, clinicians seeing little reward for the time and inconvenience associated with changing their work practice for the adoption of EHRs (van Ginneken, 2001). The human challenges involved with the implementation of EHRs were far more difficult to overcome than the technical processes.

3.1 The Patient's Perspective

While a number of authors have identified the human issues around implementation of EHRs; the majority of the previous research is concerned with the clinicians' interaction with EHRs rather than that of the patient whose record is being created and managed (Yusof et al., 2007).

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. Ensuring the privacy and security of data held on EHR systems is required to build patient trust in these systems.

Moving from a paper file record to an electronic record means that information is no longer physical but digital, and therefore more easily transportable and accessible from remote locations. Previously, 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", 2010).

Without a detailed understanding of the electronic record 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 to be strongly correlated to the level of trust they put in their providers ("Health IT Exchange", 2010., and Shield, et al., 2010). The reliance on institutional security controls alone, underestimates the importance of the provider-to-patient relationship in the formation of this trust (Shield, et al., 2010).

Health information could be considered too 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", 2010; Bauer, 2009). With the benefits of shared and accessible information there is always a price (Rynning, 2007).

The patient's trust in the privacy and security of EHRs is far more complex because these 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 of records (Alhaqbani and Fidge, 2007; Calvillo et al., 2012).

In addition to trust, Bauer (2009) raises the concept of confidentiality in relation to privacy of EHRs. The author defines confidentiality as a *"complex set of moral, social, and legal practices that work to protect ones privacy"* (Bauer, 2009, p.50). In the context of health care confidentiality is relational and based on the trust between the clinician and the patient who discloses health related information on the understanding that it is given in confidence. This concept of confidential disclosure has its roots in the Hippocratic Oath.

Traditionally the relationship between the patient and the clinician could be described as paternalistic with the clinician having complete control over the patient's record (Bauer, 2009). With the advent of EHRs, there has been a shift in power and responsibility with patients now expected in many countries to take an active role in the creation and management of their EHR (Calvillo et al., 2012).

From the literature reviewed there is evidence that there is a gap between the current institutional security measures put in place around EHRs and the patient's expectation of the privacy and confidentiality of their personal medical information. Based on the literature reviewed, the authors suggest that there is a gap between institutional and patients' perceptions of privacy and security and is illustrated in diagram 1 below.

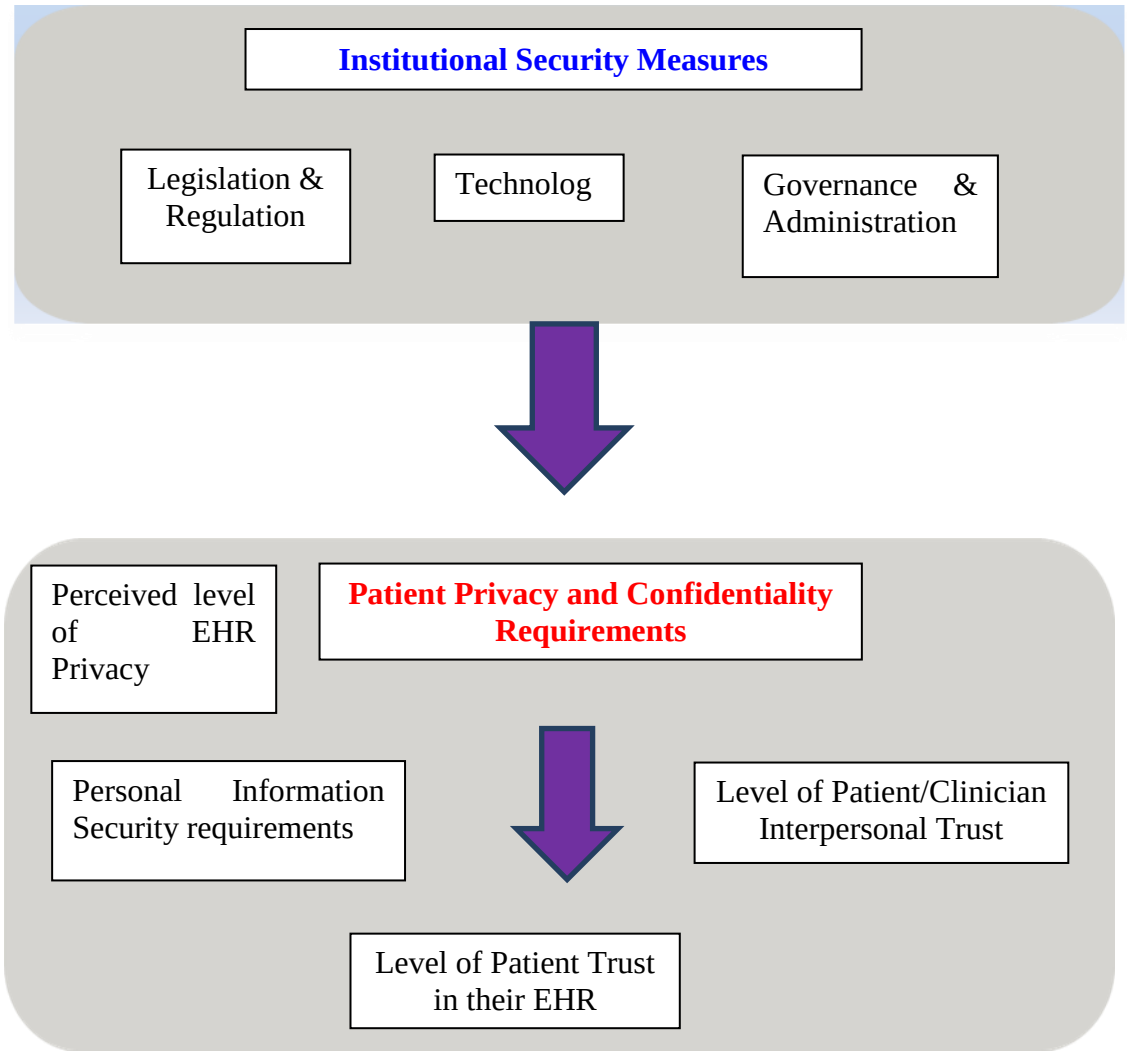

Diagram 1 - Institutional verses personal requirements for Security and Privacy

If there is a gap between the current strategies used to implement EHRs and patients' perception of the actual privacy and security of their EHR, then their lack of trust in the system may result in the withholding of vital information (FairWarning, 2011). The withholding of this information may compromise the quality of the records and the clinicians resulting trust in the information provided in the record. To investigate if there is a gap between institutional measures and patient expectations of privacy, a series of key informant interviews were undertaken.

4 Research Methodology

In order to get an overview of the issues associated with security, privacy and confidentiality, face to face key informant interviews where collected in the five countries, from e-health stakeholders, clinicians, IT administrators, government policy makers and academics. A de-

identified summary table of the key informants, their role, organisation and country of origin is listed below.

Table 1: Schedule of Key Informants

Role	**Organisation**	**Country**
Academic (Decision Support)	University Hospital	Norway
Academic (E Health Law)	University	New Zealand
Academic (EHRs)	University Hospital	Finland
Academic (Health Policy Reform)	University	United Kingdom
Academic (Regional and Remote Health)	University	New Zealand
Academic (Systems implementation)	University Hospital	Slovenia
Chief Information Officer	Regional Health Services	Australia
Chief Information Officer	Hospital Regional	Slovenia
Chief Information Officer/ Systems Engineer	Government Health Insurer	Slovenia
Client Manager	EHRs vendor	Slovenia
Clinician	Regional Health Services	Australia
Clinician	Regional Government Health Records Provider	New Zealand
Clinician (Medical Specialist)	Hospital Clinic	Norway
Clinician (Pharmacist)	Regional Health Services	Australia
Clinician (Specialist)	Hospital	Finland
Managing Director	Medical Records Software Firm	New Zealand
Minster for Health	Ministry for Health	Slovenia
Project Management	Regional Government Health Records Provider	New Zealand

Senior Policy Advisor	Government Health Ministry	Finland
Senior Policy Advisor	Government Health Insurer	Finland
Senior Policy Advisor	Government Health Records Agency	Norway
Senior Policy Advisor	Ministry for Health	Slovenia
Senior Policy Advisor	Government Health Insurer	Slovenia
Senior Systems Engineer	Private Health Insurance Firm	Finland
Senior Systems Engineer	EHRs vendor	Australia
Senior Systems Engineer	Government Health Insurance Firm	Slovenia
Senior Systems Engineer	EHRs vendor	Slovenia

The key informant research technique was selected as it has traditionally been used to develop a pattern of culture and interrelationship, and has been applied to a range of disciplines including the social sciences and business (Tremblay, 1957). In the e-health context the concepts of security, privacy and confidentiality have a relational component so key informant interviews were used to gather data that may have been difficult to obtain through structured data gathering techniques such as surveys. Wirtz et al, (2012) used key informant interviews to gain an overview of the implementation of EHRs. Clinicians were chosen as the main informants in this research due to their central role in health care provision and their influence on the attitudes of patients (Wirtz et al, 2012).

The key informants in this study were selected due to their position within an organisation and their knowledge of issues around the EHRs. These interviewees provided insights from an individual perspective on issues, which are not normally documented such as power, trust and commitment (Kumar, Anderson, and Stern, 1993). Also, key informants are most consistent when they are reporting on directly observable organisational characteristics as they were in this research (Frenk, et al., 2011).

The use of key informant interviews has allowed the authors to build up a stock of expert knowledge within the area of EHR implementation through unique insights from 'insider information' about clinical practices, software development and the policy making process (Dorussen, Lenz and Blavoukos, 2005). The complex nature of EHR implementation meant the use of key informants could provide data concerning what are often intangible variables, such as power, trust, policy development and the dynamics of interpersonal relationships. The complexity of confidentiality and privacy lends itself to being teased out through expert interviews (Kumar, Anderson, and Stern, 1993). In order to provide some level of comparison key informants were selected that held similar positions and the use of cross-cultural research was aimed at providing detailed and contrasting data (Lenartowicz et al., 2004).

The interview questions focused on the implementation of EHRs from a number of different perspectives. The interview schedule included questions relating to privacy and security issues.

1. What is the level of patient access to their records?
2. Have there been any issues in relation to information security?
3. How have you addressed the risks?

A full list of the interview questions is in appendix A.

5 Research Findings

Over the past four years, 27 key informant interviews were conducted across five countries with administrators, clinicians, information technology (IT) experts and politicians. In each of these interviews, the key informant was asked about security of the data, patient access to the records and any risks identified in the implementation of EHRs. Predominantly the interviewees discussed institutional measures for maintaining the security of patients' records. Often times in these key informant interviews IT security and administrative procedures was seen as being synonymous with maintaining of patient privacy and confidentiality.

5.1 Legal and Administrative

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 in the three European countries studied, 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. One of the respondents (a Medical Administrator, Slovenia) 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"*. In Slovenia, the Information Commissioner reviews the security of personal data held by medical providers on the EHRs. 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 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."*

In Finland, there have been standards and security level set, however these standards are difficult to enforce *"as it is hard to know the information that the Doctor needs and therefore requires access to"*. It can be seen from this comment that while laws and standards can be established for e-health and patient privacy. These processes are implemented in widely varying situations that may not match the intended regulation.

The data collected from Slovenia, Finland and Norway showed that a more centralised implementation process for EHRs led to 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, which would seem to be a common challenge (Tejero and de la Torre, 2011; Anderson, 2007).

In New Zealand, a scandal in the health sector led to the introduction of a patient's code of rights in 1996 (Health and Disability Commissioner, 2009). Under the code, patients can make a complaint to the health and disability commissioner about their treatment by the health services sector. Although the code does not specifically mention privacy, the number one right is for the patient to be treated with respect. There is far less centralisation in Australia due to a two-tiered government system (state and federal) that is responsible for the delivery of health services and the presence of a large private health sector, 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 IT vendors.

5.2 IT systems and Protocols

A common theme of the key informants interviewed was the establishment of, and subsequent reliance on IT systems to provide data security. These systems were often developed externally to the health system in which they operated. The use of external contractors meant a heavy reliance on the knowledge and skills of external systems engineers not familiar with the culture of the medical institution into which the EHR was being placed. Consistent with findings of van Ginneken, (2001) it was pointed out by a number of key informants from external IT vendors, that the systems provided were only as good as their utilisation by the medical professionals.

Finland has been running some form of electronic demographic database for the past 50 years and is currently developing a single national health database. For this database rules have been developed as to who can access what part of the data, thus providing some form of patient security. 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 access the information. The security of patient data is not seen as a significant 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"*.

Key informants from Norway, Slovenia, Australia and Finland expressed concern about the age of the IT infrastructure and the software itself. Issues discussed included, the use of personal mobile devices, the transition to web-enabled software and changing relationships with external IT vendors. For example, the text based system of EHRs in Norway does not allow for the clinician to interrogate the record, in the same manner that would be possible with a web-based system. According to one clinician interviewed, the text based system reduced the effectiveness of EHRs for patient diagnosis and management.

Predominately the deployment of multiple IT vendors and systems has led to regionalised EHR software platforms that are not interoperable. This has inadvertently reduced the risks to patients' data security and privacy associated with the electronic exchange of records. On the other hand, it was pointed by a Chief Information Officer that when patient summaries are sent to another region or medical services *"the control of information (exchanged) between external communities….there are no security checks"*. As found in previous research the respondents in this study highlighted the risk of three-way tension between IT vendors, medical administrator and clinicians creating comprise in the EHR implementation, with the clinicians often feeling like the losers (van Ginneken, 2001; Tejero, and de la Torre, 2011).

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, *"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.

5.3 Patient Perspective

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 (Deutsch, et al., 2010). Inconsistent practices around the management and input of data by clinicians was seen as a risk, 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"*. If the EHR has a poor user interface it will not be fully utilised, 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.

In most countries, patients could not access their records, except with a doctor being present. According to one Norwegian clinician interviewed, the health records are written for the Doctor's requirements and not for the patient's needs and hence could be misinterpreted if the patient was to view the record without a practitioner being present. Similar sentiments were expressed by a representative of a Finnish hospital in relation patients viewing their records as it *"will create a lot of questions for health care professionals (and) this could put health care professionals in a difficult situation raising more questions and creating more work"*. There was considerable reticence among the interviewees about allowing patient access to their EHRs. This raises the issue that if patients' cannot view their records, how can they control the information held on their record, who accesses it, and if confidentiality has been maintained.

Central to the successes of EHRs is the patient's trust in the system's ability to protect the information they supply from external access by unauthorised persons, and that the clinician will not share the information with anyone the patient does not trust. A Chief Information Officer, from a medical service in Australia, pointed out that putting in place signed consent form made patients more willing to disclose vital information. If not in place *"clinicians may not be aware of what is being withheld…or what has not been recorded due to patient's unwillingness to disclose the information. The data on the system improves as the clinicians rely more on the data and thus take more care in improving its quality. This in turn improves*

the quality of service". In New Zealand, as in Australia, GPs hold the primary medical record for patients. In New Zealand patients can ask for a hard copy summary of their record.

6 Conclusion

From the data collected there is a heavy reliance on the legal and technical means for securing EHRs in the countries examined, however the patient's perspective of EHRs has yet to be fully addressed. A recent study in the United Kingdom found that over 50% of patients would withhold information due to their privacy concerns (FairWarning, 2011). The institutional strategies for privacy and security are only part of what is required for a functioning EHR. 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, and their willingness to share information.

It is how the EHR is used by the clinician, the level of trust between the clinician, their patient and the interaction between the two, that is central to the patient's perceptions of security and privacy. As illustrated in diagram 1, a patient's trust in the privacy and confidentiality of their EHR is a multifaceted concept that technology and legislation may not be to fully address.

The point is not to downgrade the importance of having strong institutional privacy and security measure for 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, however they have to trust that what they share will be kept confidential.

With current changes in technology and rise of online social interactions the concept of personal privacy requirements in the digital realm are far from standardised or codified. According the Consumers' Health Forum of Australia (2006), there is no such thing as a standard or 'normal' patient; this is the antithesis of the institutional frameworks applied to EHRs.

Just as each patient responds differently to medical treatment, so to their privacy requirements will vary, depending on the relationship with their clinician, their personal need for privacy and their trust in the security of the EHR. With the prospect of easier and more frequently shared health data enabled by interoperable EHR systems, patients may have less control over how their records are being handled. Well informed patients who have trust in the privacy and security of their EHRs would seem to be a prerequisite for the effective implementation of EHRs. Without this trust the full benefits to themselves, their health care providers, and the health care system will not be realised.

Appendix A

Case study of e-health– Unstructured Interview Questions

1. Country?
2. Type of organisation?
3. Type of system?
4. Key features of the System used
5. System development history?
6. What impact do you think the stakeholders had on the final system?
7. Reason for adoption implementation of the system?
8. Explain the implementation process?
9. Has the system required any adaptation as part of the implementation process?
10. What was the length of time to convert to the digital/e-health system?
11. What is the level of patient access to the records?
12. How have the clinical staff, patients and the general public responded to the system?
13. What do you see as the benefits of the system?
14. Has it improved the delivery of health services?
15. How are they measured?
16. What barriers have you encountered?
17. Ways that problems were over come?
18. Ongoing issues of the system?
19. Have you identified any risks with system?
20. Have there been any issues in relation to information security?
21. How have you addressed the risks?
22. How do you see the future development of the system?

References

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

Anderson, J.G. (2007). Social, ethical and legal barriers to E-health. *International Journal of Medical Informatics*, 76, 480–483.

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

Bauer, K. A. (2009). Privacy and Confidentiality in the Age of E-Medicine. *Journal of Health Care Law and Policy*, 12, 47.

Calvillo, J., Román, I., & Roa, L.M. (2012). Empowering citizens with access control mechanisms to their personal health resources. *International Journal of Medical Informatics.* DOI: 10.1016/j.ijmedinf.2012.02.006

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

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

Deutsch, E., Duftschmida, G., & Dordaa, W. (2010). Critical areas of national electronic health record programs—Is our focus correct? *International Journal of Medical Informatics*, 79, 211–222.

Dorussen, H., Lenz, H., & Blavoukos, S. (2005). Assessing the Reliability and Validity of Expert Interviews. *European Union Politics*. 6(3), 315–337.

FairWarning. (2011). UK: How Privacy Considerations Drive Patient Decisions and Impact Patient Care Outcomes. *New London Consulting*. Available from

Frenk, S.M., Anderson, S.L., & Chaves. M. (2011). Assessing the validity of key informants reports about congregations social composition. *Sociology of Religion*, 72(1), 78-90. DOI: 10.1093/socrel/srq064

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

Health and Disability Commissioner (2009). The Code of Rights. Retrieved from http://www.hdc.org.nz/the-act--code/the-code-of-rights

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

http://www.ehealthnews.eu/images/stories/pdf/2011-WHITEPAPER-UK-PATIENT-SURVEY.pdf

Istepanaian, R.S.H., & Zhang. Y.T. (2012). Guest Editorial. Introduction to the special section: 4G Health – The long term evolution of m-health. *Institute of Electrical and Electronics Engineers Transactions on information technology in biomedicine*, 16(1).

Jha, A.K., DesRoches, C.M., Campbell, E.G., Donelan, K., Rao, S.R., Ferris, T.G., Shields, A., Rosenbaum, S., & Blumenthal, D. (2008). Use of Electronic Health Records in U.S. Hospitals. *New England Journal of Medicine*, 360, 1628-1638. DOI: 10.1056/NEJMsa0900592.

Kumar, N., Anderson, C.J., & Stern, W.L. (1993). Conducting interorganisational research using key informants. *Academy of Management Journal*, 36(6), 1633-1651.

Lenartowicz, T., and Roth, K. (2004). The selection of key informants in IB cross – cultural studies. *Management International Review.* First quarter 2004, 44(1), 23-51.

MacDermott, S., & Smith, J.R. (2013). The Future of Privacy: A Consumer-Oriented Approach to Managing Personal Data Online. *Thunderbird International Business Review* 55(1). DOI: 10.1002/tie.21520.

Mahncke, R.J., & Williams, P.A. (2006). Secure transmission of shared electronic health records: A review. *Australian Information Security Management Conference*. Posted at Edith Cowan University Research Online http//:www.ro.ecu.edu.au/ism/80

Rynning, E. (2007). Public Trust and Privacy in Shared Electronic Health Records. *European Journal of Health Law*, 14, 105-112.

Shield, R.R., Goldman, R.E., Anthony, D.A., Wang, N., Doyle, R.J., Borkan, J. Gradual Electronic Health Record Implementation: New Insights on Physician and Patient Adaptation. *Annals of Family Medicine*, 8(4), 316-326. DOI:10.1370/afm.1136.

Stroetmann, K.A., Artmann, J., Stroetmann, V.N., with Protti, D., Dumortier, J., Giest, S., Walossek, U., & Whitehouse, D. (2011). European countries on their journey towards national eHealth infrastructures - Evidence on progress and recommendations for

cooperative actions - Final European progress report. European Commission, DG Information Society and Media, ICT for Health Unit.

Tejero, A., & de la Torre, I. (2011). Advances and current state of the security and privacy in electronic health records: survey from a social perspective. *Journal of Medical Systems*, 36, 3019-3027. DOI: 10.1007/s 10916-011-9779.

Tremblay, M.A. (1957). The KI technique: a nonethnographic application. *American anthropologist, new series*, 59(4), 688-701.

van Ginneken, A.M. (2001). The computerized patient record: balancing effort and benefit. *International Journal of Medical Informatics*, 65(2), 97–119.

Wickramasinghe, N.S., Fadlalla, A.M.A., Geisler, E., & Schaffer, J.L. (2005). A framework for assessing e-health preparedness. *International Journal of Electronic Healthcare*, 1(3), 316–334.

Wirtz, B.W., Mory, L., & Ullrich, S. (2012). Ehealth in the public sector: an empirical analysis of the acceptance of Germany's electronic health card. *Public Administration*, 90(3), 642–663. DOI: 10.1111/j.1467-9299.2011.02004.x

Yusof, M.M., Papazafeiropouloub, A., Paul, R.J., & Stergioulas, L.K. (2008). Investigating evaluation frameworks for health information systems. *International Journal of Medical Informatics*, 77, 377–385.