Security and Privacy in eHealth: is it possible?

A sociotechnical analysis

Tony Sahama, Leonie Simpson
Information Security Discipline
Science and Engineering Faculty
Queensland University of Technology, Brisbane, Australia
{t.sahama; lr.simpson}@qut.edu.au

Bill Lane
Health Law Research Centre, Faculty of Law
Queensland University of Technology
Brisbane, Australia
wb.lane@qut.edu.au

***Abstract*—Advances in Information and Communication Technologies have the potential to improve many facets of modern healthcare service delivery. The implementation of electronic health records systems is a critical part of an eHealth system. Despite the potential gains, there are several obstacles that limit the wider development of electronic health record systems. Among these are the perceived threats to the security and privacy of patients' health data, and a widely held belief that these cannot be adequately addressed.**

We hypothesise that the major concerns regarding eHealth security and privacy cannot be overcome through the implementation of technology alone. Human dimensions must be considered when analysing the provision of the three fundamental information security goals: confidentiality, integrity and availability. A sociotechnical analysis to establish the information security and privacy requirements when designing and developing a given eHealth system is important and timely. A framework that accommodates consideration of the legislative requirements and human perspectives in addition to the technological measures is useful in developing a measurable and accountable eHealth system. Successful implementation of this approach would enable the possibilities, practicalities and sustainabilities of proposed eHealth systems to be realised.

Keywords—Information Security, Privacy, Electronic Health Record, Sociotechnical, Information Accountability, eHealth

I. INTRODUCTION

The term eHealth is generally used to refer to the application of information and communication technologies in the delivery of different types of healthcare services; or more directly, for the communication, sharing, retention and disposal of health information. An important application of healthcare information technology (HIT) is the provision of electronic health records (EHRs). The idea of EHRs is not new: EHRs in one form or another have been around for over five decades [1]. However, recent rapid advances in information technology; especially the development and widespread adoption of mobile electronic devices such as web-enabled smart phones, mobile devices and Personal Digital Assistants (PDAs); have changed the means by which the records can be accessed, the methods for processing the stored data, and stakeholder expectations regarding the persons who can and should have access to certain types of records.

In comparison to earlier paper-based health records systems, EHR system offer substantial benefits. Paper based records systems involve physical document storage in various locations, so information retrieval can be cumbersome and complex. However, EHRs have the potential for fast recovery, even if they are stored at a remote location. Also, with appropriate metadata, EHRs are more easily searchable. The potential application of data mining and context sensitive information retrieval techniques (e.g., natural language processing and extractions) to systems of EHRs offers further benefits. These include the potential to develop new care delivery models; performance reporting; and public health surveillance such as healthcare information exchange (HIE) [2]. The use of EHR and HIE are vital in sustainable healthcare delivery systems.

Although the potential benefits of a comprehensive EHR system are substantial, there are a number of challenges in establishing such a system [3]. For many stakeholders, information security and privacy are major areas of concern. Moreover, these concerns are especially significant in relation to the emergence of *shared* electronic health record (SEHR) systems, where information no longer resides within a single organisation. In such a situation, it is unclear how the legal obligations to provide appropriate protection for EHRs will be applied.

In this paper we explore issues related to securing SEHR systems in Australia from a sociotechnical perspective. We consider the perspectives of various stakeholders: patients, health professionals and privacy advocates in postulating a '*context sensitive health informatics*' perspective. This allows information security and privacy measures to be understood as '*human factors*' when implementing eHealth initiatives.

II. SECURITY AND PRIVACY FOR EHRs

'Privacy' is not a clearly defined concept, being subject to a number of culturally-dependent variables. In the context of EHRs, the primary concern is with the aspect of privacy referred to as 'information privacy' – a term which refers to the ability of an individual to exercise control over their personal data held by others. Information privacy concerns the collection, maintenance, use and disclosure of 'personal information': the information items that disclose the existence and identity of an individual or which could identify an individual. Examples of personal information include names, addresses, date of birth, medical records, bank account details and unique clinical identifiers such as the biological and/or physiological information of individuals.

Clearly 'health information' is a particularly sensitive subset of personal information, thus justifying the privacy concerns relating to the emergence of SEHR systems. In many countries, information privacy has been the subject of legislative regulation - generally in the context of personal information held within public and private sector organisations.

In Australia for instance, the federal *Privacy Act 1988*[4] established privacy principles governing data collection, use and disclosure, as well as data quality and data security by public and most private sector organisations, including health service providers. In relation to data security, the privacy principles impose obligations on record holders to take reasonable steps to protect all personal information in their possession from misuse and loss and from unauthorised access, modification or disclosure. New reforms to the legislation, to take effect in 2014, will broaden and consolidate the privacy principles and enhance the regulatory functions of the Office of the Australian Information Commissioner (OAIC).

Dealing particularly with data breaches concerning personal information, there is currently no specific reporting obligation under the *Privacy Act 1988* – the issue being dealt with by the OAIC in terms of what the privacy principles require in taking "reasonable steps" to protect data – usually notifying affected individuals to allow steps to be taken to mitigate the potential harm caused by a breach. However, the 2014 amendments will establish a regime for the mandatory reporting of serious data breaches as a result of loss, unauthorised access to, or disclosure of personal information and which result in a real risk of serious harm to the data subject as a result of the breach.

Alongside the general measures contained within the *Privacy Act 1988* which apply to both the public and private sector, specific federal data protection measures concerning shared electronic health records have also been enacted. The *Personally Controlled Electronic Health Records Act 2012* (Cth.) (PCEHR Act) operates in conjunction with the *Health Identifiers Act 2010* (Cth) by creating an electronic information repository of health records organised by reference to unique health identifiers allocated to Australian citizens. The PCEHR Act creates a statutory obligation to report an unauthorised collection, use or disclosure of health information or an event which may compromise the security or integrity of the PCEHR system.

Concerns about the security of information are traditionally expressed in terms of maintaining three characteristics of the information: confidentiality, integrity and availability. Providing for confidentiality means ensuring no unauthorised disclosure of information occurs. Integrity assurance involves a level of trust in the accuracy of the presented information; that it has not been subject to unauthorised modifications. Availability is the characteristic that information is provided to authorised users when needed. All of these are important for EHRs. The data security provisions, referred to above, clearly require a record holder to provide all three characteristics for EHRs and SEHRs.

In addressing the provision of data security services for information assets, it is necessary to consider the state of the information: is it in storage, in transmission (being transferred from place to place) or in use (being processed)? Each of the requirements (confidentiality, integrity and availability) should be considered for each possible information state. The appropriate mechanisms for securing information differ depending on the information state.

When considering possible measures to secure information in various states, technological solutions are frequently proposed. For example, it may be considered necessary to encrypt information during transmission in order to preserve confidentiality. Many people consider the provision of information security as solely a technical problem. However, the threats to information security are not restricted to technological sources, and so they cannot be fully addressed using only technology. It is also important to consider the interactions between people and information systems. Additional security measures relate to two aspects of this interaction: the policy and practices related to information management; and the education, training and awareness of all stakeholders in the security implications of potential actions.

The three characteristics of information, the three states of information and three classes of security measures form the basis of an information security framework [6]. A visual representation of this is based on considering the characteristics, the states and the security measures as different dimensions. Considered together, the three dimensions form a cube, as shown in Figure 1. It is useful to apply this framework to information security for EHRs, to ensure all aspects of security are considered.

Applying this to EHRs, we first consider information security aspects for information in storage. To understand the security position, how and where EHRs will be stored must be determined. For the stored records, consideration must be given to who will be granted access to the stored records, and what sort of access will be given. For example, for some users and certain fields, access may be read-only, whereas others may be able to write to or alter records. Policy regarding the record format, storage and access requirements must be established. The implementation of this and allowable practice must be established. Finally, education and training for all EHR users will be necessary, to ensure that the confidentiality, integrity and availability of stored records is not compromised by their actions. This is especially difficult in the implementation of large-scale schemes; as the user population is far from homogenous with respect to characteristics such as technical literacy; and access to and willingness to interact with digital technologies. Even within patient subgroups; such as minors, mental health patients, elderly persons, there are diverse levels of capability.

Other aspects to establish include defining the actions that are not permitted. How would a breach be determined? Who will be held responsible if the security is breached? From the technical side, to answer these questions logging and monitoring of all access will be required. This requires authentication of all users to enable accountability. This cannot be successful without the informed participation of all users. There are also associated legal issues, which are discussed in Section III and IV respectively.

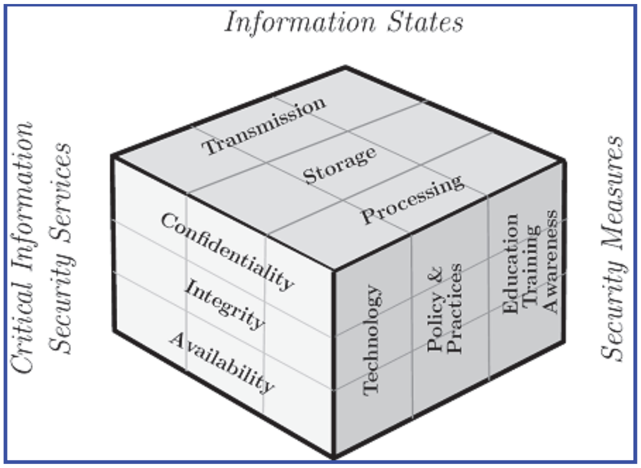

Fig. 1. Security measures for Information Dimensions[6]

When considering access to EHRs, if remote access to stored records is permitted, it is necessary to consider how the information will be transmitted between the repository and the user. What security measures can be implemented? What is the policy regarding information transmission, and what level of education and training of users is required to ensure this will not be compromised? For example, if the transmission is over insecure public networks such as the Internet, encryption will be necessary in order to ensure confidentiality. This involves the use of algorithms and secret keys. The use of resource-constrained devices (mobile phones, PDA's) for communications restricts the algorithm and key size choices. Also, compromise of the EHR system is possible if a user communicates with an insecure device; for example, a phone which has been infected with malware in a user downloaded application.

The final category of information states is information being processed; that is, in active use. To use information effectively it must be in plaintext (unencrypted) form. Confidentiality cannot be provided through the commonly used technological measures. Policy and practice and the training, education and awareness of users will be fundamental in maintaining security.

Many aspects of the implementation of EHR systems must be carefully considered in order to provide reasonable protection for personal information. Security is generally considered as a 'weakest link' problem, so the system cannot be considered to be secure unless all aspects are dealt with adequately. Given the diversity among stakeholders, many people consider this unlikely to be achieved, hence the continuing concerns over information privacy.

An alternative perspective on EHRs is to consider the implementation of EHR systems as an opportunity to achieve security and privacy protection that is greater than that available in previous paper-based systems [7], through the provision of additional functionality. This includes user authentications and authorisations, the retention of back-up files, user defined storage and retrievals and accountability measures, monitoring and logging access to records, and establishing audit trails and other mechanisms to enable information accountability [8]. Many of these measures are almost impossible to achieve at scale in paper-based systems. Appropriate access control measures can enable the potential benefits of SEHRs to be obtained while also addressing stakeholder concerns regarding security and privacy. However, it is important to realise this requires a much more comprehensive approach than an attempt to add on technological security measures to an incompletely specified and evolving EHR system. There are research challenges in providing the additional functionality while addressing the security risks associated with human behaviour through developing context sensitive sociotechnical approaches. Clearly, the diversity of the user population will require a range of strategies and incentives to deliver appropriate services for particular contexts.

III. LEGAL CONCERNS FOR EHRs

Governments in the US, UK, Canada and Australia have spent billions of dollars recently on technical aspects of eHealth implementation [9]. Yet the development of appropriate legal regulatory regimes for EHR systems, and in particular for SEHR systems, is still in its infancy. Resolving this in one country does not necessarily provide a global solution as privacy is a concept with cultural and policy variations [10].

Developing an appropriate legal and/or regulatory regime is necessary to ensure a basis for information accountability. However, despite recent legal initiatives concerning SEHRs, such as those outlined earlier, challenges remain. It is not always clear, for example, in an SEHR system, who or which entity owns or controls the records and thus where ultimate legal responsibility for information privacy resides. As well as this, coherent policies to guide the development of the information architecture are necessary to underpin effective implementation of the relevant systems. Appropriate co-ordination of measures relating to the various stakeholders (patients, healthcare providers, other data sources), requires consideration of a number of factors. Particular factors, such as the model of 'patient consent' embodied in a SEHR system, may be critical in shaping the ultimate system of legal regulation [11 & 12].

A practical approach to tackle information security and privacy challenges around SEHRs, EHR and eHealth in general, is to consider an eHealth system that is embedded with appropriate, effective and manageable information security and privacy measures and augmented by Accountable-eHealth system (AeH) protocols [12 & 13].

Contemplation of these measures should occur at the beginning of the design and development stages.

Information accountability (IA) is a concept focused on *appropriate-use* of and *after-the-fact* accountability for information usage. Transparency and the presence of accountability mechanisms are necessary to build trust in the system and are also expected to act as a deterrent for intentional misuse. eHealth systems built to follow the principles of IA are called Accountable-eHealth (AeH) systems [13]. Figure 2 illustrates the role of IA in the eHealth domain. In this scenario, observe how patients' healthcare information might flow in the eHealth environment.

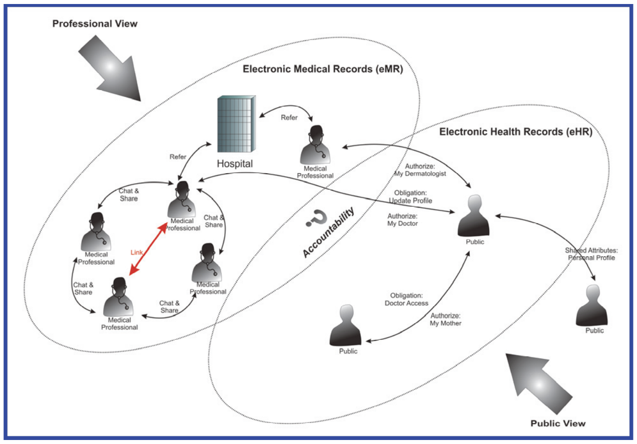

Fig 2. eHealth Scenario[8]

The flow of information between the professional and public domains must be monitored to control the way in which data is used by HCPs, and to assure the public of the security of their sensitive information. The monitoring mechanism can be implemented as an information accountability framework (IAF). The three main aspects of the IAF: Legal, Social and Technological and their interrelationships are shown in Figures 3.

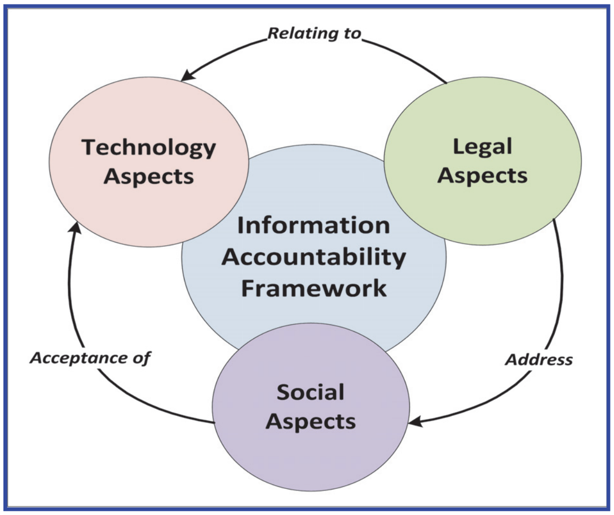

Fig 3. Information Accountability Framework[12]

Accountable eHealth systems rely on appropriate legislation for the governance and regulatory mechanisms to be established. A case study of the Australian eHealth system identified that, in its current state, the existing Australian legal foundations are inadequate for implementing the regulatory mechanisms necessary for AeH systems to function as intended [12]. In Australia, the Federal *Privacy Act 1988* (Cth) states the principal measures relating to information privacy. However, the effective development of AeH systems in the Australian context depends upon the establishment of an appropriate underlying legal framework to adequately address a range of specific issues including information ownership, access and control, data breach notification and broader issues involved in the legal management of the system as a whole.

The recent enactment of the *Personally Controlled Electronic Health Records Act 2012* (Cth.) to operate in conjunction with the *Health Identifiers Act 2010* (Cth), is designed to address these issues by creating an electronic information repository of health records organised by reference to unique health identifiers allocated to Australian citizens. Along with recent amendments to the *Privacy Act 1988* (Cth), introducing measures such as mandatory data breach notifications; these developments provide a more comprehensive legal foundation for the emergence of an effective AeH system. These are advances but the implementation issues remain unresolved.

IV. eHEALTH PROCESSES AND PROTOCOLS

While the process of converting existing physical health documents and medical records to digital versions or copies has begun, the development of effective large scale systems of EHRs is still a long way off. Public awareness and acceptance of EHRs is limited and the involvement of professionals (such as clinicians and healthcare decision makers) in this EHR journey varies around the globe. In many places, the owners or custodians of the medical/health data and information (e.g., PCEHR or PHR, EMR and EHR) are not yet clearly identified. It is important that a physical person (e.g., human) is responsible for the contents of the digital document (e.g, EHR, EMR & PHR). The integrity and non-repudiation of these EHR documents and/or processes may be affected by the actions of the responsible person. Addressing this represents an ongoing challenge in both HIT policy and the related legislative debate.

In general, information processing and timely information exchange is important in disseminating quality information to enable effective and efficient clinical decision making. In the digital healthcare setting, information sharing at the individual and institutional levels is critical to enable valid informed clinical decisions making. At the same time, as noted in section III, sharing health information and extending access to personal records presents a risk; there are security and privacy concerns and legal challenges that must first be addressed. The relationship between the benefits and the risks can be indirectly measured on the basis of trust between healthcare professionals and the public.

To better understand the information flow between public and professionals in a given eHealth scenario, we present a graphical view of SEHR in a sociotechnical perspective, by integrating a human dimension (Figure 4). This graphical depiction has global application, without prejudicing country specific legal and/or legislative protocols.

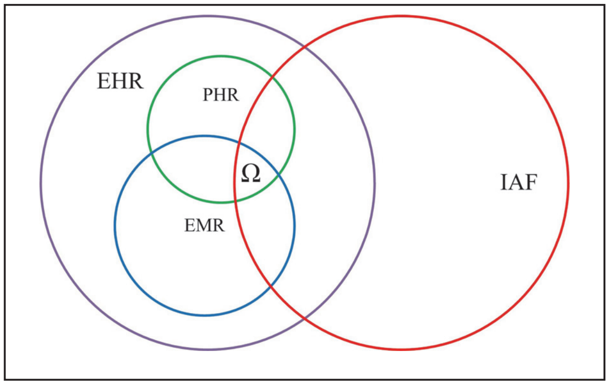

Fig 4. Graphical view of SEHR in sociotechnical perspective [15]

While there is no universally accepted definition for the term eHealth, an EHR is the building block of an eHealth system, combined with personal health records (PHR) and other aspects, these PHRs are referenced as Personally Controlled EHR (PCEHR), and electronic medical records (EMR). The relationship between PHRs, EMRs and EHRs is a complex data structure. However, the use of an IAF to monitor the information security and privacy aspects, together with legislative requirements should provide sufficient scope for the inclusion of human aspects and behaviours.

PHR: is recognisable, individual information stored, collected, shared and controlled by individual (the public view)

EMR: is amended, updated PHRs that managed by authorised clinicians and healthcare organisation (the professional view).

We argue that an eHealth system should be designed to support improved healthcare services and/or to enhance the quality of clinical decision making processes. Such an eHealth system should consider the "**critical pivotal point**" (intersection of PHR, EMR, EHR and IAF, marked as Ω in Figure 4), seriously, from the outset of system design and development. We observe and hypothesise, such interconnections comprise with human behaviour, information flow, [for example, the state of the information: is it in storage, in transmission (being transferred from place to place) or in use (being processed)], and information accountability measures are aspects the majority of eHealth systems have failed to address [16].

A number of different regulatory models exist in relation to the privacy and security of EHR data and information – evident, for example, in the Health Information Technology for Economical and Clinical Health Act 2009 [17]; the Health Insurance Portability and Accountability Act (HIPAA); the European Data Protection Directive 95/46/EC, as well as various specific legislative initiatives. While regulation is important, accountability requires the implementation and use of certain technical approaches; symmetric key and/or asymmetric key schemes, pseudo anonymity techniques in EHR systems, digital signature scheme based on PKI (Public Key Infrastructure) where the ID and key are bound with digital certificates; use of a PIN or biometric measures. The security of all of these measures depends on the interaction of people with the technology. These human dimensions are critical and helpful with sociotechnical validity.

V. DISCUSSION

In summary, health information exchange (HIE) is a powerful tool [2] with the capacity to make a significant and positive difference in healthcare delivery. At the same time, it depends upon an appropriate legal regime, valid information and privacy measures, and the deployment of strategies to deal with human factors to strike the correct balance in relationships between the relevant institutions and individuals themselves, and ensure that individuals are not disempowered. Sustainable healthcare processes must take account of and effectively manage the risks concerning the privacy and security of the relevant information.

We presented an argument that technology, social and legal aspects (Figure 3) using human involvement must be considered when designing and developing eHealth systems. The juxtaposition for our hypothesis is based on sociotechnical perspective and possibilities for implementing secure eHealth system. Different countries will have different legislative approaches. Ultimately, however, the evolution of appropriate and sustainable EHR and eHealth systems requires a collective and integrated approach based on appropriate policies, and accountability measures. Implementing appropriate information accountability measures requires specific attention to the data use agreement, in particular, the control of information access. The way forward lies in recognising and addressing the issue as "context sensitive" processes involving "human factors."

VI. CONCLUSION

This paper explores issues related to information privacy in the context of measures being adopted for shared EHR systems in Australia.

EHR and SEHR systems must be designed so as to enhance security and minimise breaches. This is especially so in the case of SEHR systems where issues of access and use accentuate security concerns. Despite legislative initiatives designed to enhance security and minimise breaches, such as those outlined earlier, the integrity of records cannot be achieved through the application of technology alone and is especially difficult in large-scale schemes with a diverse user populations.

We approach these issues from a sociotechnical approach - considering the perspectives of various stakeholders: patients, health professionals and privacy advocates in order to form a '*context sensitive health informatics*' perspective. This approach is based on understanding information security and privacy measures as '*human factors*' when implementing eHealth scenarios.

In this context, important issues concerning SEHR systems includes such matters as who owns or controls the records or where the ultimate legal responsibility for information privacy resides. The development of an appropriate legal or regulatory regime to deal with shared records is necessary in order to enable information accountability mechanisms to be developed. Information accountability mechanisms which monitor user actions and compare the information flow with defined appropriate usage models are envisaged as a deterrent to intentional misuse. In other words, there are three main aspects of the Information Accountability framework: Legal, Social and Technological. The interrelationship of these must also be considered.

VII. FUTURE DIRECTIONS

The challenges concerning the emergence of EHR and SEHR systems centre on ensuring a regime sufficiently capable of utilising the technological benefits involved in accessing and sharing electronic records which also embodies sufficiently enhanced security measures. Developing a workable access and accountability framework is interconnected with the adoption of appropriate legal measures of regulation. For the most part, the legal initiatives undertaken thus far remain untested. The extent to which they sufficiently address the challenge of EHR and SEHR systems remains to be seen as a matter requiring future study.

ACKNOWLEDGMENT

Authors would like to thank Randike Gajanayake for preparing the graphics and proof reading of the manuscript.

REFERENCES

[1] E. D. Acheson, “Oxford Record Linkage Study: A Central File of Morbidity and Mortality Records for a Pilot Population”, Brit. J. Prev. Soc. Med, vol 18, pp. 8—13 (1964).

[2] A. Adler-Milstein and A.K. Jha, “Sharing Clinical Data Electronically: A Critical Challenge for Fixing the Health Care System”, JAMA, 307(16), pp. 1695—1696, 2012.

[3] R.E. Hoyt and K.G. Adler. Electronic Health Records. (https://www.practicefusion.com/resources/InformaticsEducationChapter3.pdf — Retrieved on 25 April 2013).

[4] Australian Privacy Act 1988 (Cth)

[5] Australian Privacy Act 1988 (Cth) and 2001 Amendment (Cth)

[6] NSTISSI. “National Training Standard for Information Systems Security (INFOSEC) Professionals, NSTISSI No. 4011, 20 June 1994

[7] W.R. Hersh. “Medical Informatics: Improving Health Care Through Information”, JAMA, vol 288(16), pp. 1955—1958, 2002.

[8] Randike Gajanayake, Renato Iannella, and Tony Sahama, "Sharing with Care An Information Accountability Perspective," Internet Computing, IEEE, vol. 15, pp. 31-38, July-Aug. 2011.

[9] D. Protti, and IB Johansen, “Widespread Adoption of Information Technology in Primary Care Physician Office in Denmark: A Case Study”, Issues in International Health Policy, The Commenwealth Fund Pub. 1379, vol 80, pp. 1—13, 2010.

[10] P. Chhanabhai, and A. Holt, “Consumers are ready to accept the transition to online and electronic records if they can be assured of the security measures”, Med Gen Med, 9(1), pp.8, 2007.

[11] World Health Organization, *Legal frameworks for eHealth: Based on the findings of the second global survey on eHealth* (2012) Global Series on eHealth, vol 5, 9-12.

[12] R. Gajanayake, B. Lane, R. Iannella, and T. Sahama, "Legal issues related to Accountable-eHealth systems in Australia," presented at the 1st Australian eHealth Informatics and Security Conference (AeHIS), Perth, Australia, 2012

[13] R. Gajanayake, R. Iannella, B. Lane, and T. Sahama, "Accountable-eHealth Systems: The Next Step Forward for Privacy," presented at the 1st Australian eHealth Informatics and Security Conference (AeHIS), Perth, Australia, 2012.

[14] D. Benyon, J. Preece, Y. Rogers, H. Sharp, S. Holland, and T. Carey, "Human-Computer Interaction," ed: Addison-Wesley: Reading, MA, 1994.

[15] Gajanayake, Randike, Sahama, Tony R., and Lane, William B. “The Role of Human Factors when Evaluating Information Accountability for eHealth Systems”. In *Context Sensitive Health Informatics Conference*, 18-19 August, 2013., Copenhagen, Denmark. (In Press)

[16] T. Sahama, and Miller, E. “Informed use of patients' records on trusted health care services”, International Perspectives in Health Informatics, Volume 164 Studies in Health Technology and Informatics, pp, 127—131, 2011

[17] A. K. Jha. “Meaningful use of electronic health records”. *JAMA: the journal of the American Medical Association*, 304(15):1709-1710, 2010.