Context Sensitive Health Informatics: Human and Sociotechnical Approaches
M.-C. Beuscart-Zéphir et al. (Eds.)

doi:10.3233/978-1-61499-293-6-97

The Role of Human Factors when Evaluating Information Accountability for eHealth Systems

Randike GAJANAYAKE[a], Tony SAHAMA[a,1] and Bill LANE [b]
[a] *Science and Engineering Faculty, Queensland University of Technology (QUT), Brisbane, Australia*
[b] *Faculty of Law, Queensland University of Technology, Brisbane, Australia*

Abstract. The availability of health information is rapidly increasing; its expansion and proliferation is inevitable. At the same time, breeding of health information silos is an unstoppable and relentless exercise. Information security and privacy concerns are therefore major barriers in the eHealth socio-eco system. We proposed Information Accountability as a measurable human factor that should eliminate and mitigate security concerns. Information accountability measures would be practicable and feasible if legislative requirements are also embedded. In this context, information accountability constitutes a key component for the development of effective information technology requirements for health information system. Our conceptual approach to measuring human factors related to information accountability in eHealth is presented in this paper. Measuring the human factors associated with information accountability can benefit from extant theories from information systems research and business management. However, the application of such theories must clearly address the specialised nature of the application context coupled with the role of the users within the context.

Keywords. eHealth, eHealth requirements, Information privacy and security, Information accountability, Human factors methodologies, protocol and policy evaluation

Introduction

eHealth socio-eco systems deal with human health and behaviour. They require timely and effortless access to healthcare information [1]. However, healthcare information is a particularly sensitive form of personal information, usually subject to more onerous forms of legal regulation than personal information generally. Nonetheless, potential information privacy and security threats to patient information can be minimised by providing proper technology and implementing measurable tools of user behaviour, mitigating the risks. At the same time, information privacy and information access requirements give rise to competing concerns that require critical attention by systems designers, vendors, policy makers and practitioners if systems are to have the expected positive effect on healthcare delivery. The challenge is to strike the appropriate balance between protecting the privacy of patients whilst retaining access by authorised healthcare providers, especially where there exists a serious threat to the safety of the

[1] Corresponding Author: Tony SAHAMA. Email: t.sahama@qut.edu.au

patient or the community generally. Achieving a correct balance has proven difficult. As a solution for this conundrum and as explained in an earlier paper, an Information Accountability Framework (IAF) has been proposed for eHealth systems [2], which encompasses social, technical and legal dimensions. The successful implementation of eHealth systems based on IAF protocols and policies depends upon a careful evaluation of all relevant IAF dimensions.

Systems are evaluated in a number of ways. These include model checking, prototyping and usability testing by human factor methodologies. The entire software engineering lifecycle can be considered in the evaluation process that principally involves requirement analysis, system design, implementation and testing. Although technical and functional aspects can be evaluated with well established methods [3], evaluating non-functional protocols and policies of a system is a difficult task given how they affect end user behavior and performance. The above mentioned evaluation techniques allow system designers to test the systems functionality, and performance although the underlying policies and protocols cannot be validated as such.

Identifying the effects that system protocols and policies have on the users is a key consideration for eHealth systems. However, selecting the correct methodology and evaluating these effects are not straight forward tasks. As Dale Carnegie (1888 - 1955) states, "[when] dealing with people, remember you are not dealing with creatures of logic, but with creatures of emotion, creatures bristling with prejudice, and motivated by pride and vanity". The field of human factors can greatly contribute to eHealth systems in their design, implementation, and evaluation phases.

This paper aims to understand the role of human factors in evaluating the non-functional aspects of the IAF designed towards information privacy management in eHealth systems. The details presented here are not a result of a systematic review of literature but a starting point for such a study and a point of view of the authors that would lead to a more extensive study in the near future.

1. Information Accountability Framework

The IAF builds upon information accountability principles and facilitates appropriate use of healthcare information by HealthCare Professionals (HCP). The presence of after-the-fact accountability measures seeks to ensure that policies and rules of information use are followed by the end users. This is considered preferable to enforcing rigid restrictions on information access – something which is deemed unsuitable for a specialised and knowledge driven domain such as healthcare.

eHealth systems that are built with the IAF as the foundation have been coined Accountable-eHealth (AeH) systems [4]. AeH system protocols have been designed with the aim of ensuring that patients have control of their healthcare information stored in Electronic Health Records (EHR) and that such information is accessible by patient-nominated HCPs. The idea is that whilst access and use of information in EHRs is generally to be governed by principles of information privacy, this should not, in itself, prevent HCPs from accessing information they professionally judge is required for making informed decisions towards better healthcare delivery for the patient or, in some circumstances, the community. In terms of the overarching legal regulation of EHRs and as the practice in different jurisdictions shows, this can be based on varying types of organisational governance involving differing levels of information management and based on different consent (or 'opt in') models. Irrespective however

of the exact method of legal regulation, transparency and accountability within the controlling EHR institution is critical for the operation of effective information governance principles [5]. In AeH systems, transparency and accountability can be achieved by giving patients the capacity to inquire about possible misuse of their information by HCPs – thus acting as both a deterrent against intentional misuse and an incentive to abide by the rules. It also acts as a means of enforcing non-repudiation, which is a central concept of information security. Continuous misuse of information by users is prevented by revocation of policies that can be built into the system with a predefined threshold.

The underlying protocols and policies of AeH systems are defined in the IAF with related technical, legal and social dimensions. The technology aspects [2; 6] and legal requirements [7] for the implementation of AeH systems have already been demonstrated. The social aspects of the IAF remain to be evaluated using appropriate measures in accordance with the thesis of this paper. As indicated above, the measurement of the social aspects using human factor methodologies is seen appropriate given the nature of the IAF and the effect human behavior has on eHealth systems in general.

2. Human Factors

Methods of human factor analysis can be categorised into two principal groups depending on their place in the systems development life cycle: methods used for user centric design and methods used for system evaluation. Commonly used methods in the field of human factors, specifically in eHealth, include techniques such as paper prototyping and sketching, thinking aloud, scenarios and storytelling, interviews and field studies, questionnaires, logging and other observation methods, simulation and modeling, analysis of video and mediated communication, modeling and analysis of communication processes [8]. These methods contribute either to one or both of those two groups.

It is important to make a clear distinction between the concept of usability engineering and human factors relating to non-functional aspects of a system. Usability engineering is a principal area of human factors that focus on the functional aspects of a system. Usability can be defined as a measure of ease of use and usefulness of an information system in terms of its effectiveness, efficiency, enjoyability, learnability, and safety [9]. But non-functional aspects such as protocols and policies, which are key drivers of the IAF, require methods that can capture the relationships between how individuals react to protocols and policies introduced by a system.

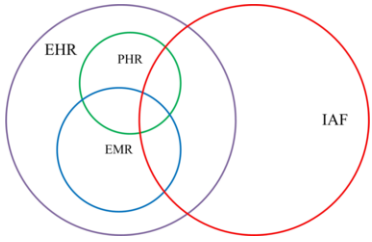

Figure 1. Relationship between eHealth and the IAF.

eHealth systems utilise three main types of information sources: Electronic Medical Records (EMR), Personal Health Records (PHR) and EHRs as the main information resource. Overlaps exist between them as depicted in Figure 1. Information manipulation of EMRs and PHRs can be identified as professionally controlled and patient controlled respectively where as in EHRs it is shared between the professional and public domains. As depicted in Figure 1, the IAF targets the portion of EHRs, EMRs and PHRs that involves human interaction. Therefore, its effects on the functionality of EHRs, EMRs and PHRs can only be measured through the use of human factor methodologies that are catered to capture the respective user requirements and activities. This becomes more complex with EHRs due to the shared control.

3. Human Factors and the IAF

Human factors studies in the context of the IAF must include a clear distinction of the professional and public domains. As mentioned above, the requirements of the professionals and the patients in an eHealth system can give rise to competing concerns whereby a balance can only be reached with trade-offs. But these trade-offs can have direct effects on the way end users perceive the deliverables of a system. Information privacy is as crucial a requirement for patients as information access is for HCPs. The human factors contributing to the nature of the requirements of each stakeholder must be recognised.

The healthcare domain is a dynamic environment that needs to cater for different types of healthcare stakeholders with different levels of capabilities and expectations. For example, the eHealth domain must take into consideration the effect 'digital natives' and 'digital immigrants' have on system protocols and policies. Although eHealth is considered to be a great strength in the treatment of elderly patients, they, being 'digital immigrants', are the least likely to readily embrace eHealth systems [10].

4. A Model for Investigating Human Factors in the IAF

An attractive approach to evaluating non-functional aspects of the IAF in terms of human factors is empirical research models of user behaviour from the closely related fields of information systems research and business management. Several empirical models have been successfully used in measuring the contribution of human factors in the adoption and proliferation of information and communications technology in the healthcare domain [11]. These models focus on either the professional domain (i.e. healthcare professionals) or the public domain (i.e. patients/consumers). However, a clear distinction between the roles of the users within the system domain has to be made considering the nature of the interaction with the system. The dimensions of specific measurements play different roles concerned with the different parties involved. For example, patients prefer and expect to have control of their healthcare information maintained in EHRs [12]. But HCPs may not always agree. Similarly, the notion of holding users accountable may have inverse effects on system adoption within each user group. Attempts to accommodate such differences can be seen in the varying types of 'consent models' (referred to earlier), utilised as part of the governance system for the particular form of legal regulation chosen for EHR management [13, 14].

Our initial investigation into the development of measurement and structural models for the IAF revealed relationships with theories such as technology acceptance models, theory of reasoned action, expectation disconfirmation theory and the theory of planed behaviour. It is important to consider four main contexts: individual, technological, implementation and information as seen in Figure 2.

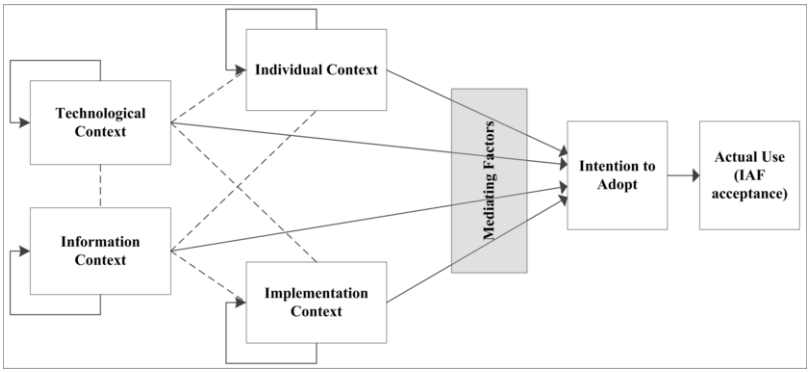

Figure 2. A model for investigating the role of human factors in IAF acceptance.

Figure 2 shows the relationships of each context with the intention to adopt the IAF, with each other (shown in dotted lines) and internal relationships. The individual context will examine the impact of aspects related to technology acceptance that are personality traits such as anxiety and attitude towards technology. The technology context will capture data related to what users expect the technology to deliver in terms of job performance and effort, two well known constructs from technology acceptance literature and in the healthcare technology domain [11]. The implementation context captures aspects related to organisational facilitating conditions, social influence and suitability of the technology with the work environment, which have been previously tested and validated in the healthcare domain [11], but not in the IAF context.

Most important to the IAF, the information context consists of constructs that capture aspects relating to: 1.) information accountability: the users' perceived belief that accountability measures must be present in eHealth, 2.) information control: the users' perceived belief that patients should have control of their healthcare information and 3.) information governance: the users' perceived belief that the use of information must be governed by predefined rules in eHealth systems. These constructs focus on the non-functional policies and protocols of the IAF, which have not been empirically tested in information systems, business or healthcare domains.

The model will measure the relationships between these perceived beliefs and the intention to adopt the IAF with the presence of mediating factors yet to be incorporated into the model. In accordance with prior research [15, 16], we theorise that a user's intention to adopt a system is positively correlated to actual use, which cannot be empirically tested without implementation. Depending on the user domain, the relationships between each context may either be positive or negative and would have different effects on each other and on the intention to adopt the IAF. Therefore, each domain needs to be evaluated separately. Through empirical investigation, the aforementioned effects can be identified and remedies can be made to minimise negative effects towards system adoption.

5. Closing Remarks

Human factors play a significant role in the evaluation of the non-functional aspects of eHealth systems and therefore in the evaluation of the IAF. Appropriate measures and methods must be taken into consideration when developing measurement instruments for evaluation. A possible approach is to adopt theoretical research models available in the field of information systems and business management capable of measuring the relationships and effects of systems protocols and policies on consumer adoption and use of technology. However, the application of such theories must clearly address the specialised nature of the healthcare domain and the IAF coupled with the role of the users within the context.

References

[1] A. Shaban-Nejad and V. Haarslev, Human Factors in Dynamic E-Health Systems and Digital Libraries, in W. Pease, M. Cooper, R. Gururajan (Eds.), *Biomedical Knowledge Management: Infrastructures and Processes for EHealth Systems*, ISR Series, IGI Global, 2010, 192-202.

[2] R. Gajanayake, R. Iannella, and T. Sahama, An Information Accountability Framework for Shared E-Health Policies, in: *WWW2012 Workshop on Data Usage Management on the Web,* L. Kagal and A. Pretschner, eds., Lyon, France, 2012.

[3] B. Kitchenham, O. Pearl Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, Systematic literature reviews in software engineering–A systematic literature review, *Information and Software Technology* **51** (2009), 7-15.

[4] R. Gajanayake, R. Iannella, B. Lane, and T. Sahama, Accountable-eHealth Systems: The Next Step Forward for Privacy, in: *1st Australian eHealth Informatics and Security Conference (AeHIS),* P. Williams and L. Coles-Kemp, eds., Perth, Australia, 2012.

[5] L. Kloss, Information governance: the essential accountability wrapper, *Health Data Management* **20** (2012), 97.

[6] R. Gajanayake, R. Iannella, and T. Sahama, An Information Accountability Framework for Shared E-Health Policies, in: *WWW2012 Workshop on Data Usage Management on the Web,* L. Kagal and A. Pretschner, eds., Lyon, France, 2012.

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

[8] G. Demiris, N. Charness, E. Krupinski, D. Ben-Arieh, K. Washington, J. Wu, and B. Farberow, The role of human factors in telehealth, *Telemedicine and e-health* **16** (2010), 446-453.

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

[10] T. Heart and E. Kalderon, Older adults: Are they ready to adopt health-related ICT?, *International Journal of Medical Informatics* (2011), e-pub ahead of print.

[11] L. Schaper and G. Pervan, ICT and OTs: A model of information and communication technology acceptance and utilisation by occupational therapists, *International Journal of Medical Informatics* **76** (2007), S212-S221.

[12] S. Haas, S. Wohlgemuth, I. Echizen, N. Sonehara, and G. Müller, Aspects of privacy for electronic health records, *International Journal of Medical Informatics* **80** (2011), e26-e31.

[13] H. Deutsch and F. Turisco, Accomplishing EHR/HIE (EHEALTH): Lessons from Europe, *Strongsville, OH: CSC Healthcare Group,* 2009.

[14] P. Kierkegaard, Electronic health record: Wiring Europe's healthcare, *Computer Law & Security Review* **27** (2011), 503-515.

[15] P.Y.K. Chau and P.J.H. Hu, Investigating healthcare professionals' decisions to accept telemedicine technology: an empirical test of competing theories, *Information & management* **39** (2002), 297-311.

[16] W.G. Chismar and S. Wiley-Patton, Does the extended technology acceptance model apply to physicians, in: *System Sciences, 2003. Proceedings of the 36th Annual Hawaii International Conference on*, IEEE, 2003, p. 8 pp.