1-1-2014

Changing Places: The Need to Alter the Start Point for Information Security Design

Elizabeth Coles-Kemp
Edith Cowan University

Patricia A. Williams
Edith Cowan University

eJHI electronic Journal of Health Informatics
www.eJHI.net
2014; Vol 8(2):e13

Changing Places: The Need to Alter the Start Point for Information Security Design

Lizzie Coles-Kemp[1] and Patricia A H Williams[2]

[1] Information Security Group, Royal Holloway University of London, UK
[1] School of Computer and Security Science, Edith Cowan University, Joondalup, WA, Australia
[2] eHealth Research Group, School of Computer and Security Science, Edith Cowan University, Joondalup, WA, Australia

Abstract

Information security is a necessary requirement of information sharing within an electronic health system because without it confidentiality, availability, or integrity controls are absent. Research shows that the application of security in this setting is subject to workarounds partly because of resistance to security controls from clinicians who feel that their voice is excluded from the security design process. Heeks' explored the nature of health system design and referred to the distance between system designer and practitioner as the 'design-reality gap'. To reduce this gap, systems designers typically deploy user-centred, participatory approaches to design. They use various forms of consultation and engagement to ensure that the needs of users are responded to within the design and that users understand the design process and constraints. Whilst there is evidence to suggest that the overall electronic health records (EHR) system design has increasingly used elements of a participatory, human-centred design approach, the security elements of design are still technology-focused. This discussion paper characterises the problem, outlines the principles of Heeks' Information, Technology, Processes, Objectives, Skills, Management Systems, Other Resources (ITPOSMO) framework, and then uses this framework to evaluate security dimensions of both the UK and Australian EHR programmes. The resulting proposal for a 'communities of practice' approach as an alternative start-point to healthcare systems security design, provides a basis for reconceptualising the integration of security practices into EHR systems. In the increasingly distributed and complex environment of healthcare delivery, this new approach can help to address the fundamental challenges experienced in healthcare security practice today.

Keywords: Information Security; Participatory Design; Electronic Health Records; E-health

1 Introduction

Electronic health record (EHR) systems are notoriously difficult to design, and designing secure EHR systems is an even harder task. Part of the difficulty lies in the fact that the actual electronic health record is not simply the conversion of paper records to digitised form but is often a re-engineering of healthcare services. This re-design often takes advantage of an EHR's ability to 'push the boundaries' of healthcare [9] and to allow transformation of the approach to the cycle of patient care. From a security perspective, the EHR is not simply a static data asset with one set of security attributes. EHR technology enables the record to be used to document the health of the patient in any number of contexts, turning the record into a ubiquitous asset with dynamic security requirements. This ubiquity means that the data's value can change as the patient's care needs change. For instance when a patient is in an acute state access to information is critical and often the need to share information cannot be pre-planned as access requirements are in response to the change in the patient's condition and can not necessarily be predicted. As a result, security functionality has to respond to the dynamic care practices that the

clinical staff adopt; responding to this within system design is complex, particularly as care practices vary from one community of health practitioners to another.

The problem in designing secure EHR systems is sometimes characterised as a gap between the reality envisaged by systems designers and the reality envisaged by system users. This type of gap is sometimes termed a 'design-reality' gap [3]. In healthcare, one manifestation of the design-reality gap is clinical workarounds [4], and workarounds in the EHR environment include clinical staff retaining stores of local copies of medical records because the EHR system is not trusted. Some would argue that workarounds are inevitable, a fact of everyday design [43]. If workarounds are considered as a part of everyday design, a form of design in-use, workarounds can be seen as an act of appropriation, an act of reclaiming control over a process or system. However, from an information security perspective these workarounds create spaces where information sharing is not governed or controlled by the security functionality or management framework. One example of a security-related workaround is the sharing of a login-session on a patient record system in order to avoid the overhead of logging off and logging on. This workaround is rationalised in many ways, a common argument being that it saves time and effort, or that all members of the clinical team trust each other. Indeed, in a hospital environment to enforce the regime of logging on and logging off with individual credentials places significant and prohibitive workflow demands on the healthcare team. Regardless of the rationalisation, the log-on and off example is still a workaround that resists the design of the access control system and this is a significant resistance because, in design terms, access control functionality sits at the heart of the EHR and is the basis on which digital records are shared. This login-sharing workaround creates a gap that can be exploited to subvert the access control system and gain unauthorised access to health information or to make unauthorised changes to the healthcare records. In order to close this gap, security designers could analyse the existing methods of data access and consider methods of digital sharing that are more culturally sympathetic. It should be noted that from a security perspective, minimising the design-reality gap reduces the possibilities for exploitation that can ultimately affect patient safety and therefore design processes that reduce this gap are an important step in securing EHR systems.

Academic Richard Heeks has used the Information, Technology, Processes, Objectives, Skills, Management Systems, and Other Resources (ITPOSMO) framework when evaluating the success of new healthcare system implementations. In his analysis, Heeks points out, health information systems have a history of being difficult to design and implement successfully [3] and indeed, it is difficult to define either success or failure of such a system because they are complex and often part of large programmes for change. Large national programmes are particularly difficult to categorise. For example, in 2010, significant parts of the UK's National Health Service IT Scheme were cut [5] and over the following 12 months, the focus moved away from electronic healthcare systems that were designed and deployed from the centre to systems that were developed and implemented at local level [6]. However, it would be wrong to characterise this programme as a failure. A number of successful EHR systems did emerge from this programme, including the NHS Spine (a national database of summary records), Choose and Book (a service where patients can choose where to receive medical treatment) and the Picture Archiving and Communication Service (PACS). This success is quite possibly because the systems more closely met the needs of the target user communities and demonstrably improves the quality of clinical care. These successful systems are deployed in primary or secondary health care across the country and are valued by clinical staff and patients. Nevertheless, the original UK plan for a centrally designed and deployed EHR system was not wholly successful and many of the problems cited in the programme reviews [7, 8] reveal many of the design-reality gap dimensions articulated by Heeks' ITPOSMO framework.

Heeks [3] identified that the design-reality gap is often caused by the designer's lack of understanding of the realities in which the users operate and by the users' lack of understanding of the design realities. Both sides of this gap can be seen in the responses to the Royal College of Nursing's e-health survey in 2007 and 2010 [10, 11]. The Royal College of Nursing is supportive of EHR systems and recognises the benefits such systems can bring [10] but also acknowledges the challenges of implementing and using these systems. In order to bring about these benefits, Heeks suggested that perhaps a more participative approach to EHR design might reduce the gap and in many ways this is indeed the direction of travel that EHR design has taken. Certainly, there is a trend towards a user-centred and a more participative approach to EHR system design (and indeed public systems in general) but as the UK and Australian examples demonstrate, this trend does not appear to have reached the information security aspects of EHR design. This paper uses Heeks' lens to explore why information security aspects of EHR are particularly prone to the design-reality gap and to identify the barriers that need addressing to close that gap.

To date little use has been made of Heeks' ITPOSMO framework to analyse specifically the design of security functionality in a system, and this paper demonstrates the value that such analysis can bring.

2 The Design-Reality Gap

Heeks identified seven dimensions to the design-reality gap [3]. These gap features are also termed the IT-POSMO dimensions. These dimensions are points at which a gap can appear between the reality that the system was designed for and the reality in which a system is implemented. These dimensions are:

- Information - for example the system was designed to produce one type of information but there is no need for that type of information.
- Technology - for example the system requires one type of technological infrastructure but the healthcare organisation has another type of infrastructure.
- Processes - for example the system is designed to automate decision-making processes but these processes are very different to the pre-system ones that are still in operation.
- Objectives and values - for example the system prioritises formal records and the clinical team prioritises clinical relationships that deploy informal information sharing techniques.
- Staffing and skills - for example the system requires a particular level of technical expertise and confidence that is not present within the system's target user group.
- Management systems and structures - for example the system requires a level of formal sign-off for the increase of system's rights but authorisation for increase to access rights is informal within the user setting.
- Other resources - for example there is a significant overhead and effort required to learn how to use the system and the clinical staff have very little time to adopt these new skills.

Heeks suggested that a participative approach might help to close the gap along each of these dimensions. Gaps in any one of these dimensions can influence the degree to which the implementation of the system is deemed a success. Heeks' dimensions clearly articulate the position that a health information system is a socio-technical system and not purely a technical system. It follows therefore that a participative design approach would not only contribute to the technological parts of a system but also to the social and organisational parts. In healthcare to date, this has been a significant and difficult problem to address [12]. The argument often put forward by participatory designers is that where system design is technology-centred rather than practice-centred, a gap emerges that is filled by disengagement, and resistance practices. This gap and the response to it can open the way for security breaches where the attacker exploits weaknesses in information management practices. Security reports routinely show [1] that weak information management practices are one of the largest root causes of successful attacks and EHR systems are not exempt from weak security management leading to successful attacks [2].

The notion of design participation is strong in Human Computer Interaction (HCI) research. Vines et al [44] describe participation in the following way: "The term 'participation' is traditionally used in HCI to describe the involvement of users and stakeholders in design processes, with a pretext of distributing control to participants to shape their technological future." Vines et al. go on to point out that the notion of participation is very strong within the HCI community, noting that some 115 papers in the ACM's 2012 Computer Human Interaction Conference (CHI 2012) included the term 'participatory'. It is an approach that has its roots in the principle of democratisation of the design process and the active involvement of the end-user in shaping the technologies of their future. Vines et al. claim that, whilst retaining its traditional roots, HCI has developed the concept to also include means of distributing decision-making processes across an organisation or communities and creating active involvement in creative processes and knowledge sharing activities. Despite this increase in scope, the notion of participatory still has links to the philosophy of increasing user control of the design process and of the resulting technology. The degree of participation depends on the participative quality of the engagement; at one end an engagement can be more passive and essentially participative in nature and at the other end of the scale, active engagement can be seen as truly participatory. Whilst users have long been recognised as important participants in the analysis of security issues [15, 45], the notion of users taking an active role in the design of security technologies is not one that is typically included in current security design approaches. Instead, the focus of user participation [15, 45] tends to be in the design of the security management and implementation frameworks using risk and audit methodologies not in the design of the underpinning security technologies. To follow Heeks' suggestion of

participative engagement requires an active involvement of users in the conceptualising of the goals of the security system, the values embedded within the security technologies and the form the technical security controls assume.

Heeks' dimensions offer a lens through which to analyse the challenges in implementing the security system element of an EHR system. For example applying the ITPOSMO framework to information security and EHR might yield the following potential gaps:

- Information – the system was designed to produce one type of system log and alert information for system activity but the system log and alert events are not relevant to the operation of the clinical environment. Consequently, the system alerting function is not used as part of the management practices.

- Technology - the system requires one type of user account management infrastructure and authentication system but the healthcare organisation has a different, more low-tech, infrastructure for managing both and as a result work-arounds appear for sharing user accounts and passwords.

- Processes – the system is designed to automate the processes for assigning access to medical records but these processes, and the decisions that are made, are very different to the pre-system socially-based processes that are still in operation. As a result, work-arounds appear to share data in ways that circumvent the access and auditing systems.

- Objectives and values – the system prioritises formal authorisation in assigning access rights and the clinical team prioritises a sharing of tasks that requires informal access. The impact of which is that formal authorisation is only provided for audit purposes and is not perceived as a useful practice.

- Staffing and skills – the system requires a particular level of technical expertise and confidence in order to administer the access rights to the electronic health records that the clinical team using the system does not possess. As a result, aspects of the EHR system are not used, or confident users informally perform tasks on behalf of less confident users, resulting in an erroneous or incomplete audit trail of record usage for clinical tasks.

- Management systems and structures – the system requires a level of formal sign-off for the increase in access to electronic health records, but authorisation for increase to access rights is informal within the clinical team with the potential result that formal records are not up to date and the audit trail does not reflect the actual authorisation for changes.

- Other resources – there is a significant overhead and effort required to learn how to use the security features of the system and the clinical staff have very little time to adopt any new skills. Consequently, poor system practices evolve and resentment towards the system's security controls increases.

As can be seen from the examples above, the Heeks' dimensions require us to evaluate the security design from the perspective of the designers and from the target user community, rather than from the perspective of the data or the technology as is more usual in security design. As a result, the ITPOSMO framework triggers analysis that looks at the combination of both the security technologies and the management of those technologies from the perspective of those using and designing the system.

To gain a better understanding of the issues across national health systems, two national examples of EHR programmes, the UK EHR programme and the Australian Personally Controlled Electronic Health Records (PCEHR) programme, were selected. These two programmes were chosen because of the different positions that these programmes take on the role of the central health department and because the Australian programme followed on from the UK programme [13, 14] with a greater emphasis on participative design. In the analysis of these national examples, the Heeks' dimensions are used as a lens through which to make sense of each programme.

3 The UK Approach

In order to evaluate the UK programme, the House of Commons Public Accounts Committee report from 2007 and the House of Commons Health Committee report from 2007 were examined as part of this research. In addition, the 2007 and 2010 e-health surveys commissioned by the Royal College of Nursing were analysed. From these reports, an analysis using the ITPOSMO framework was conducted.

The UK's EHR system programme was subject to considerable public scrutiny. Numerous reviews were undertaken and subsequently reported. A persistent theme in the reports is the perception from the clinical 'front-line' that the system had been imposed on them.

For example, the 2007 report from the House of Commons Committee of Public Accounts shows that much effort was made to engage and consult with clinicians and yet there are reports of the perception 'on the front line' was that the system is misaligned with the clinical requirements. The 2007 report presents the following as one of four key findings:

> "The Department has much still to do to win hearts and minds in the NHS, especially among clinicians. It needs to show that it can deliver on its promises, supply solutions that are fit for purpose, learn from its mistakes, respond constructively to feedback from users in the NHS, and win the respect of a highly skilled and independently minded workforce." [7]

Using Heeks' dimensions, the above quote can be interpreted as a gap between the objectives and values espoused in the system design and those found on the clinical front-line. This type of gap is one in which resistance activities can build up posing problems for security managers and compliance officers as well as potentially damaging the quality of the care records.

The Committee's 2007 report goes on to state that the decline in popularity of the system, evidenced through the UK's Royal College of Nursing surveys between 2004 and 2007, was a result of poor planning, poor organisation and poor engagement with clinicians. This further emphasises the depth of the perception that the system was imposed top down and arguably illustrates a lack of confidence in those commissioning and managing the implementation of the system. The UK's Royal College of Nursing had commissioned surveys since 2004 on their memberships' views and perceptions of EHR and these surveys provide a valuable documentation of the perceptions as they evolved amongst nursing staff. The surveys show that confidence in the system did increase between 2007 and 2010 and concerns about patient confidentiality slightly reduced.

Whilst the 2004 and 2007 the Royal College of Nursing surveys did not measure the perception of system implementation and design, the qualitative responses to this effect were sufficient to be referred to in the Commons Select Committee report of 2007. The qualitative interview answers appended to 2010 survey results shows that gaps in terms of processes, staffing and skills and management and structures was felt to be present:

> "I think that little recognition has been given to nurses using technology but doing so 'invisibly' within the clinical system [...] The emphasis on the hardware seems to be at odds with what the nurses want from technology and such an emphasis alienates nurses from discussing how they feel about technological change in a clinical setting... [10](p.27)."

In terms of the framework, this gap can be interpreted as a staffing and skills gap and a processing gap as the information management practices that exist within this community are culturally, rather than technologically, focused and do not naturally move to a technological focus. The gap description above reflects the overall technology focus rather than the human-centred practice focus.

This gap is further articulated in this response in the 2010 survey:

> "The money that has been invested has been wasted – IT has been developed by people who do not fully understand clinical roles and therefore the systems do not enhance clinical practice... [10](p. 28)"

This extract further highlights the perceived gap between the information management practices that predate the EHR system and those that the EHR system attempts to foster.

3.1 Security Aspects of the UK EHR Design

Security is integral to how healthcare information is used and shared and is a fundamental aspect of patient safety. The design-reality gap can also be identified in the descriptions of the security design aspects of the EHR system found in the reports of the House of Commons reviews from 2006-2007. For example, the House of Commons Committee of Public Accounts report from 2007 indicates that security concerns were raised and highlighted as part of the review process. The quotation below illustrates the socio-technical nature of the security system:

> "Another issue that has prompted concerns amongst doctors and others is the protection of patients' confidentiality, where Dr Nowlan told us that the most important issue was the arrangements for governance and trust, and compliance with these arrangements. The Department told us that the security systems in place will be more secure than the Chip and PIN arrangements utilised by credit and debit cards in the UK. It was also supporting the Information Commissioner in his demands for higher penalties for information abuse." [7](p. 21)

The technology of the security system, 'more secure than the Chip and PIN arrangements', has the potential to introduce, in some implementations, a process gap by introducing an authentication token that changes the way in which clinical staff accessed systems. How this change is responded to potentially affects the safety of the patient. If the changes are not accepted, then workarounds emerge and the integrity of the system is challenged.

The importance of maintaining the security of these systems is clearly outlined in the Summary of the House of Commons Health Committee report entitled 'The Electronic Patient Record', Sixth Report of Session 2006-07. It is interesting to note that the problem is framed as a technical one and there is recognition of the potential for issues if the technology is implemented without careful attention to clinical process change to accompany the technical system implementation.

> "Maintaining the security of the SCR (summary care record) and NCRS (NHS care record) systems is a significant challenge. Each SCR will potentially be available across the country to a wide range of users, making operational security especially problematic. Connecting for Health, the organisation responsible for delivering NPfIT (National Programme for Information Technology), has taken significant steps to protect operational security, including strong access controls and audit systems. However, the impact of these measures in the complex environment for the NHS is difficult to predict. We recommend a thorough evaluation of operational security systems and security training for all staff." [8](pp.3-4).

The same report identifies that the EHR system brings new risks, particularly to privacy and safety of health information (p.7) and the report outlines the security requirements (pp. 36-41). Whilst the report outlines both the technical security requirements and the human factor or operational security requirements, it is noticeable that the operational requirements in this report focus on enforced change. In the challenges and criticisms section of the report a number of issues are raised about the difficulties of implementing the operational security. In particular, it is noted that the complexity of clinical roles might make role-based access control techniques impractical for the healthcare environment (p.40). Fundamentally to the debate, Dr. Martyn Thomas is quoted as arguing that security systems did not appear to have been designed with users in mind:

> "...in deciding what the specification for the technology should be, you actually need to start by looking at the specification of the overall social system and deriving the specification for the technology out of the way that people are genuinely going to behave when faced with the technology" The moment it appears to them that systems are getting in the way of doing their job which they see as treating patients and running the hospital effectively, they start working around the systems." (p. 41)

It can be seen from this quote that gaps and resulting workarounds were regarded by some as inevitable. It could be argued that workarounds appear in response to the attitude of enforcement and top-down management. Information security is often the subject of a 'strong culture' mentality where the culture of security is pushed onto an organisation in a top-down manner. It has long been recognised that successful information security management approaches are ones in which all members of the organisation are engaged [15]. The premise that underpins this belief is that information security affects all members of the organisation and therefore everyone must engage with its control. However, the terms of engagement and the manner of engagement is controlled by organisational security cultures that are, almost invariably, implicitly top-down rather than sub-cultural, or ground-up [16]. The philosophy of the strong culture approach is that

> "effective top managers could build a strongly unified culture by articulating a set of 'corporate' values, perhaps in a vision or mission statement. If those values were reinforced consistently through formal policies, informal norms, stories, rituals, and jargon, in time almost all employees would allegedly share those values" [19] (p. 8).

Examples of this implicit approach can be found in numerous information security management writings on policy design [17, 18].

This process of reinforcement is typically part of the process of embedding policies within an organisational unit. The intention is not necessarily one of enforcement; the intention is often that the organisational units will locally adapt the governance approach to fit their operating contexts. However, the reality is often the reverse because centrally managed security policy compliance processes might result in organisational units feeling forced to adapt their processes to fit the governance structure [20]. One of the main reasons for this is

the technology-led design culture of information security, which uses technology to drive process and practice change from the centre. This tradition of strong culture and of a technology-centred culture potentially helps to explain why information security design is often a process that produces design-reality gaps and repeatedly generates environments in which many security workarounds evolve.

4 The Australian Approach

It is currently too early for significant feedback in the use of the PCEHR since its introduction in July 2012. Whilst to date reportedly 1.3 million people have registered for a PCEHR, there are only 13,000 healthcare summaries uploaded and no publicly available statistics on the usage of or access to these summaries [42]. Indeed, the disquiet and discontent with the PCEHR resulted in a government inquiry into its use in late 2013, for which the future of the PCEHR is yet to be decided. In contrast to the UK analysis in the previous section that was based on reports from a matured process of formal reviews, the basis for the Australian analysis in this section is on the design approach as it relates to the outcomes of the Heeks' framework, rather than on a comparison of the outcome of implementation. However, this extrapolation of the design to outcomes provides a useful indicator of the potential resultant effects that may be seen as adoption and use of the national ehealth system increases.

A primary issue that emerges from the analysis of the Australian case is that of delineation of responsibility for the delivery of the ehealth system as a series of components, namely the infrastructure, implementation, and use. In 2005, the Australian, State, and Territory governments, to develop better ways of electronically collecting and securely exchanging health information, established the National E-Health Transition Authority, known as NEHTA. Whilst NEHTA [21] has a vision 'to enhance healthcare by enabling access to the right information, for the right person, at the right time and right place', this vision does not specifically include implementation and use. The issue with this approach is that it is information focused and does not prioritise how the information will be used as a cornerstone of the development of the infrastructure that it is supporting.

In comparison to the UK approach, the development of Australia's new e-health system has employed a limited participative approach to the technology and architecture design, with the use of tiger teams, community consultation, and clinical lead engagement [22]. A "tiger team" is a group of experts assigned to investigate and/or solve technical or systemic problems [22] and there was a bias of technical staff in such teams which diluted the participation from front line users. The use of such teams can speed up the process of development of the standards required and gives ready to access professional and expert advice in the community. However, the approach to the security aspect of Australia's e-health, both point-to-share and point-to-point, still reflects the traditional top-down, strong culture approach. The security design was derived from taking the specialist approach to the issues of security rather than from the participation of front-line clinical staff. The tiger teams involved in the security aspects of the PCEHR only involved those with security expertise and did not include clinical staff, nor consider the clinical workflow integration of security with the diverse processes in clinical use of the record. This positions security as a technical specialism and not a system dimension that can be designed by non-technical specialists. The consequence of this positioning is a lack of determination of how security processes can be integrated seamlessly into clinical utility workflow. A risk approach is not inclusive of the design as it is an 'after the fact' activity identifying risks and finding mitigations for them. This is effectively outside the design of the initial solution.

As an overarching framework, designed to be embraced across the healthcare sector, a National eHealth Security and Access Framework (NESAF) was developed [23]. This development also included consultation with security experts. From the higher-level engagement perspective, it is clear that a design-reality gap also exists in the development of the NESAF. Whilst the value of ehealth process patterns to the management of security is recognised in this risk-based asset identification framework, nonetheless a framework imposes the technologically driven security processes onto, rather than integrated with, this process workflow. For instance in the NESAF

> "The [ehealth process] patterns are also useful in developing risk treatments, as they provide a context within which the assets need to be managed....They can also help organisations consider the people, process and technology interactions and data flows associated with their eHealth activities" [24](p.17).

This indicates that organisational clinical workflow can be applied but is not central to the development of the ehealth process patterns. It could also be argued that analysed through Heeks' framework this 'after the fact' positioning of security could be interpreted as resulting in a gap in processes, and staffing and skills. Further, the specification that:

> "Process models are deliberately represented at a high level, to enable healthcare organisations to recognise the overall relevance of the pattern in their organisation. As such, they do not reflect alternate scenarios or pathways, but rather that process through which most successful transactions will pass. It anticipated that organisations may need to further develop business process models including the flow of data within and outside of their organisation in order to fully analyse the risks and compliance points for their organisation" [24](p.18),

highlights how it is expected that the processes will simply fit into the technological system that is proposed rather than be designed to form a socio-technical system.

> "Each ehealth process pattern outlines the key, high level steps, commonly involved in the process, and includes numbered linkages to specific Security and Access Components where relevant" [24] (p.18).

Instead of being developed as true collaboration, the e-health process patterns, and the integration of the security into these patterns is left to each organisation to devise for themselves. This clearly demonstrates a potential design-reality gap in multiple aspects of Heeks' framework, including the management systems and structures aspect.

In the development process, the national body, NEHTA [21] cites collaboration as a key factor in its engagement strategy. Whilst there were some 700 encounters with stakeholder groups through meeting, conferences, and workshops, most of these were forums for information provision rather than participative collaboration and design encounters [24]. The essence of the tiger team approach, whilst participative, was aimed at technical design of solutions for the ehealth infrastructure and conformance. It could be argued that this limitation is consistent with the NEHTA vision, but falls short of what is required to implement and use a national e-health system. In addition, the adoption of the tiger team was late in the development cycle. The approach did not focus on engagement of primary users for integration into workflow and were more technical in nature. The approach targeted data processing capabilities such as healthcare identifiers, authentication and access control, secure messaging, clinical terminologies and information, supply chain, pathology requests and reports, diagnostic imaging requests and reports, medications management, referrals and discharge summaries [24]. Applying Heeks' framework to this approach would widen the target of analysis to include user-focused elements including influence processes, objectives and values, staffing and skills, and other resources. The engagement of stakeholder groups so late in the development, and specifically the omission of clinical specialists in the security development, means that these wider, user-focused elements were not included. This lack of focus potentially means that the management systems and structures will lack the oversight and inclusion of clinical involvement. This is a serious potential omission, given that it is the clinical team who will be undertaking, and expected to engage in, the security function.

The Australian response shows the perspective of security design is still more technology than culturally-centred [26], with little engagement on aspects of management or governance, and work practices. Whilst the overall approach in Australia has increased stakeholder consultation [27] the security design aspects of the initiative were still approached in a technology-centred manner using subject matter experts and did not solicit engagement by front-line clinical practitioners. Indeed, whilst there were some 450 stakeholders engaged in the system design during the 700 encounters, the process mainly involved identification of the barriers and challenges, risk and opportunities of a personal EHR rather than the design of the clinical workflow, and security and access elements [27]. This raises the concern that whilst system design engagement of this type aims to be broad and inclusive, in the Australian case it was predominantly aimed at consumer and care provider adoption and designed to meet government and political requirements and tight timeframes, as evidenced by the NEHTA PCEHR Specification and Standards Plan [22]

> "To enable the progression and accelerate the adoption of eHealth through infrastructure integration and standards for health information"(p.13), and "The tight timeframes for the development and delivery of the PCEHR System, balanced against NEHTA's strategic priority to lead the development of eHealth Standards, mean that a new optimised and connected process is required" (p.20).

Unfortunately, this type of approach is often inadequate when it comes to capturing the requirements and issues related to in-depth information use, workflow, and security. Subsequently, this can result in a superficial functionality design framework in terms of integrating working practices and technology. In the Australian

case, the interests of the lobby representing the consumers of healthcare heavily influenced the design of the system in relation to privacy and patient access to the PCEHR. This drove the design to focus on the consumer control (privacy and controlled access) and resulted in the opt-in system [28]. Such an approach is not fully participative, as the interests of one stakeholder group drives design over the interests of another. In addition, this approach has as its start-point, information and systems, and not the target user community themselves. In this case, the consumer rights and protection lobby backing, together with the technical impetus, dominated the design process and healthcare practitioners and the 'clinical front-line' had less representation in this aspect of the architecture. This imbalance is reflected in the design of PCEHR that prioritises one set of stakeholder requirements over another.

As the Australian shared EHR is still in its infancy, it is too early to make comment on the alignment with clinical requirements however it is clear that research will be needed to provide the clinical utility of the system and provide evidence to the healthcare teams who may use it. This view is supported by the initiation of the recent government inquiry so soon after the introduction of the PCEHR in mid 2012. From the perspective of information security, the Tiger Team 'expert' design approach to security meant that the reality of integrating security into clinical process remains a gap. The assumption is that the user community will be able to put effective measures into practice. This does not take into account the additional demands on healthcare providers, particularly those at the end-points of the healthcare systems, such as primary care and specialists. Recognition of this is evidenced by the work of professional associations in developing their own standards for assisting the clinical fraternity to practically apply and integrate security practice into clinical and administrative workflow [47]. It is unfortunate that this has been a necessity, as the resulting security solutions for the national EHR system do not integrate with the already complex process of workflow in healthcare.

5 Community of Practice: an Alternative Start-Point

Many of the gaps described in the two national example applications of Heeks' framework in the previous sections reflect a misalignment with the cultural practices of clinical teams and the information management practices expected/enforced by the technical EHR system. Heeks suggested that a more participative and user-centred approach to systems design might help to close such design-reality gaps. A user-centred design approach seeks to reduce the design-reality gap by positioning the design from the perspective of the end-users of the system and by developing approaches that facilitate and enable dialogue between different stakeholders in the design process [29]. Research has demonstrated that in the healthcare environment, the strong top down approach causes a gap between expected and actual clinical practices [30]. This is partially attributable to the devolved accountability from management to frontline healthcare staff, such as administrative staff and practice managers, who have had less input as stakeholders to the systems they are expected to adopt and use. Devolved accountability means accountability for the impact of day-to-day data management now sits with frontline staff rather than with senior management. Although these staff are not regarded as a major stakeholder in the EHR design process, they are the ones who will engage in the security processes on a day-to-day basis. As a result, the systems do not necessarily align with the healthcare practice goals of frontline clinical staff. In particular, systems that focus on specific information goals do not easily support information sharing and access requirements that occur on the frontline. Networks of practice develop within a work place and can operate counter to the design of data and information security mechanisms, thus highlighting the design-reality gap. Including the networks of practice into the design of a system offers a different perspective on information sharing and access, and places the focus on the user-community rather than on the data and the technology. This moves the focus away from individual design needs and onto collective design needs.

Networks of practice are referred to commonly as 'communities of practice' and offer an interesting alternative start-point to healthcare systems design. If a community of practice focus is adopted in the design process, the cultural practices related to information sharing and access would naturally be uncovered as part of the system requirements phase, thereby reducing the gaps identified through Heeks' framework and the worked examples. Eckert [31] suggests that communities of practice "emerge in response to common interest or position, and play an important role in forming their members' participation in, and orientation to, the world around them". This is an important factor when considering the development, adherence to and promotion of information security practice. Wenger [32] defined communities of practice as "[...] groups of people who share a concern or a passion for something they do and learn how to do it better as they interact regularly". This intrinsically includes the process of information sharing, and applies to anyone who is engaged in a "shared

domain of human endeavour".

Whilst having its roots in linguistic anthropology and social stratification, communities of practice provide a valuable perspective with which to investigate groups within an organisational developmental environment [33, 34]. Fundamentally, the proposition is that community of practice learning, and subsequent change, is derived from social experience [35]. Lave and Wenger [34] refer to this as 'situated learning'. Extrapolating this concept to the development of security culture, it is clear that situated learning is analogous to contextualisation of social practice within a specific environment. A key element of this is the fluidity of the social space and the diversity of experience within the environment in which the community of practice functions [31]. Indeed since communities of practice materialise from engagement in common goals or interests, they are fundamental to the participation and perception of the environment in which they operate. As a result, any design process that takes communities of practice as its focus must be a participative process that studies the requirements in their context of use, because communities of practice only exist within the environment within the environment in which they operate. Such an approach would naturally produce culturally sympathetic systems, adapted to individual environments.

5.1 A Community of Practice Approach to Security Architecture Design

A community of practice approach to understanding the context of system use in terms of the information practices, information-sharing values, and the tacit agreements that a community builds around information sharing, supporting a system design approach that is inclusive of its system users. In particular, such an approach may reduce the type of gaps identified in the national examples.

A community of practice view is rooted in the notion that "The real technology is the human resource available to hospitals, homes and social health organizations" [36]. Hence, a framework is needed to explore and interpret how this human technology can interoperate with EHR systems. This is something that Dr. Martyn Thomas called for when he stated, "you actually need to start by looking at the specification of the overall social system and deriving the specification for the technology out of the way that people are genuinely going to behave when faced with the technology..." [8](p.41) One sociological approach to achieve this outcome is to use a theoretical framework to support and interpret the interplay of technology and social activity. A number of approaches exist such as Normalization Process Theory (NPT), to explain the adoption, or lack of adoption, and level of integration into routine practice that new technologies had in e-health [37]. Whilst not explored further here, NPT addresses the gap between research and application, and focuses on 'implementation and integration of interventions into routine work (normalisation)' [38]. Approaches such as NPT are often operationalised through a process model which looks at the impact a complex system implementation might have on a community's information management practices, how community members relate and share knowledge with other community members, and the effect a complex system implementation might have on these relations. The analysis also considers the way in which skills and workload are shared and how the complex system implementation might affect this, together with its impact on the context for the community.

In order to operationalise such an approach within design, it is important to consider how a community of practice needs to be supported by technology. Wenger [32] suggests that to support a community of practice you need to recognise:

- the domain - the identity of the shared commitment and competancy of the group;
- the community- (the relationships that the domain members posess; and
- the practice - the shared resources, experiences and ways of dealing with problems.

These characteristics will define the shift in paradigm to support improved adoption of security management practices in healthcare. The integration and adoption of common practice is derived from contextualised practice and is not readily adopted if that knowledge is decontextualised, abstract, or general [41]. This requirement drives the design process to being participative and results in systems that adapt to different environments and drivers.

5.2 A Case Study in design through communities of practice in information sharing

A published study in the application and engagement with information security in primary care [12] considered how communities of clinical practice needs to be supported in the advent of technological EHR. The research explored actual practice with electronic records in primary care; issues and barriers; and perceptions of information security, as represented in Figure 1. The study identified communities of practice for information sharing and management in place within primary

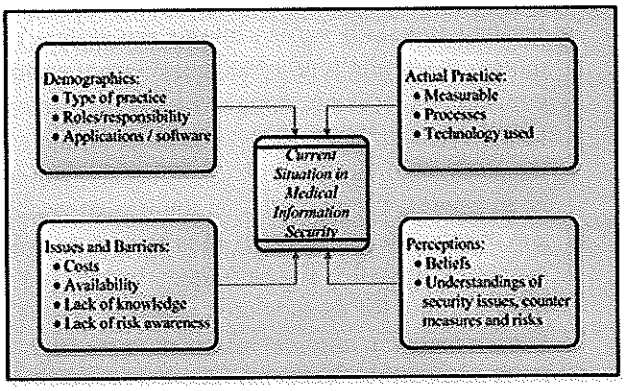

Figure 1: Competing factors in information security [46]

care, and from this understanding developed a security governance model called Tactical Information Governance Security (TIGS) model, which is sympathetic to the working practices, found in the communities of practice that the research uncovered. This study reflects a design process that is user-centred rather than technically centred and engages with rather than imposes on existing communities of practice within the healthcare environment.

In order to develop the TIGS design, data was collected from in-depth interviews about current processes, beliefs and the working environment of the general practices selected using the NPT framework to understand the existing communities of practice and the potential impact of EHR technologies. The authors of this paper used data collected from this study in order to construct an example of analysis using Heeks' ITPOSMO framework and to explore how a communities of practice approach might be operationalised. This study was selected because it focused on primary healthcare in both the UK and Australia, and the data relates to security practices and associated perceptions and this is the focus of our study.

The study [12] had concluded that the characteristics that influence information security in practice in primary care are trust, capability, cost, time knowledge, poor implementation, attitude, and inconsistency in implementation. In our study, we re-ran the exercise of evaluating patterns of practice against Heeks' framework using the data from the primary healthcare environment study in [12]. This exercise yielded the following design-reality gaps:

- Information – *for* example, the system was designed to produce one type of information but there is no need for that type of information. The data in [12] demonstrated that this could occur where there is a lack of control over the information produced and its relevance to the target environment. In healthcare, particularly primary care, trust is a major factor inherent in the environment. This includes trust in software and its reporting. Whilst designed to provide information on security performance and issues, the manner in which information related to security is communicated is incongruous with the understanding of the user. This information gap is also due to the fundamental issue for the user of why the information is even required. For the user there is a perception that there is 'no need' for this information as trust in the information systems and their security would make this unnecessary. In the healthcare environment, a lack of knowledge of the use or implication of security related to the information presented is a significant and important gap. This aspect of Heeks' framework suggests that the design-reality gap is from both the user and the design perspectives. The user trusts that the systems are doing what is required to protect them, yet the security solution provider assumes that the user is proficient in what to look for and what action to take with the information produced.
- Technology - *for* example, the system requires one type of infrastructure but the healthcare organisation has another type of infrastructure. The data in [12] demonstrated that information security solutions assume levels of infrastructure that are not in existence in all levels of healthcare. The major force behind this is that 'clinical costs outweigh security concerns' and therefore priority and justification for infrastructure is a disparity between the design of solutions and the reality of what is implemented to support security solutions. Further, the costs for infrastructure including fundamental security processes such as checking the reliability of backups, is a restriction to security practice: 'Checking the restore backup more than quarterly incurs greater cost'. The expectation of the security profession is that this is done at each backup or at least weekly. This is only one example of this type of gap.
- Processes – *for* example, the system is designed to automate decision-making processes but these processes are very different to the pre-system ones that are still in operation. In software applications, particularly of a clinical records nature, there is an assumed predictive consistency in process by the user. The data in [12] illustrated that this is rarely apparent. For instance, whilst accepted (by security professionals) that it is good security practice to change passwords periodically, the decision

process for this is left to the individual medical practice and individual to put into effect. It is rarely enforced by organisational governance practice, and most primary care systems do not enforce this. The underlying assumption, in the design of such system aspects, is that the user process will drive this security process. This is a gap between good security provided by supporting software and user activity. The inconsistency and discrepancy in expectations is perceptible where uses acknowledge that 'Good practice is constantly monitoring, can't rely on computers to do that, but practice does not do any monitoring'. It also highlights the failure in process where 'No plan for system unavailability' occurs. Given that security practice comprises a significant human element, this affects both the development of a security culture as well as the level of effective security in place.

- Objectives and values – for example, the system prioritises formal records and the clinical team prioritises clinical relationships and the informal information that is shared. Analysis of the data in [12] highlights that a strong culture of trust exists in healthcare environments. The perspectives in use of information systems and the security of the system are not shared perspectives by designers and users. This is demonstrated by the complex set of relationships that the clinical user needs to maintain, with support from the information system as secondary. The security solution provider cannot encompass or demand specific process and procedure, and has a clearly defined data and technology centred view of the solutions. This usually means that the solution is expected to be used and managed in a certain way; however, this is a major issue that is affected by other aspects of Heeks' framework including staffing and skills, and management systems and structures. For instance, attitudes articulated in the interviews towards the use of security highlights the incongruence of system objectives and community values. For example: 'They [patients] appreciate that you've got well organised notes but they don't really care you know so it's only for our convenience so you have to balance out how much money do you want to spend on high tech stuff vs the good old patient interaction because sometimes it can be quite interfering with the way we do things especially with slow typers etc. Also, 'clinical procedures more important than backup and security'. There are strongly defined gaps in shared objectives between security system design and the target user community.

- Staffing and skills – for example the system requires a particular level of technical expertise and confidence that is not present within the clinical team that form the system's target user group. As the analysis of the data in [12] shows, this aspect is an important contributor in the design-reality gap of implementing security in primary care. The capability of staff is raised frequently and significant training for users is seen as being required to even maintain minimal information security "I think some of the issues are that user issues i.e.; the capabilities of some of the staff". The basic design-reality gap here is the lack of intuitiveness and seamless inclusion of security measures into underlying systems. There is a 'Need to educate staff more as everyone has access to the internet' and 'A lot more we could do on the training aspect'. The presence of this gap, particularly in security solution design, influences security practice and the ability to ensure a secure information environment.

- Management systems and structures – for example the system requires a level of formal sign-off for the increase of system's rights but authorisation for increase to access rights is informal within the clinical team. The security knowledge level of those responsible for implementing and maintaining security is an important issue to address in primary care as shown in [12]. This is across the gamut of information security from governance such as awareness and knowledge of legal responsibilities, to understanding of what security technologies provide. This is compounded by the responsibility for security being allocated to the senior administrative person, usually the practice manager. The role of technology and its operational responsibilities are assumed to be understood by the security solution providers, yet in reality these are not commonly well defined, and not allocated to people in the environment based on expertise but seniority. Given the view that 'day to day issues come before security' it is reasonable from a healthcare perspective to place some reliance on the security solution providers to take account of this user perspective. For instance, whilst audit trails are provided as part of the security features in software applications, access level restriction and more importantly the ramifications of these, are omitted and there is little inherent control over these features: 'IT and security [are] a priority only when they fail'. Clearly, strategic oversight and governance needs to be in place for such management systems and structures to flow down to the operational level and

close this design gap.

- Other resources – for example there is a significant overhead and effort required to learn how to use the system and the clinical staff have very little time to adopt any new skills. A significant issue for clinical users is the constraint on time as the interviews in [12] show. This is reflected in many security measures being postponed or never undertaken. 'Time is a prohibiting factor in security implementation' and there is 'no time to monitor staff on Internet' and 'no time to cull user access list'. What is required is 'simple, straightforward communication on Security and IT knowledge'.

Overlaying Heeks' design-reality gap framework with research into computer and information security in primary care [12] presents an example of how the framework relates to the current methods used to design and implement information security in practice, as only once facet of health information systems. The analysis highlights the gaps that emerge between practice and technology design when the security framework and technology do not reflect how the communities of practice resolve the tensions between the demographics, the issues and barriers, the actual security practices and the security perceptions.

In attempting to address and control some of these design-reality gaps, the TIGS model offers an alternative means of identifying security requirements [46]. The model is instantiated through a capability maturity assessment tool that contains a series of techniques and methods that enable the base lining of current practices from where security practices that were sympathetic to not in conflict with those practices could be developed. Williams [46] describes the modifications that were made to the information security governance framework for primary care and the results of the model evaluation. The introduction of this capability tool enables the identification of information that is needed by the communities of practice in operation amongst front-line clinical staff. It situates any system needs within the values and objectives of the target community of practice. In order to do this, the capability tool identifies the current day to day management practices within the community of practice itself that pertain to information management and sharing. Further, the tool identifies the technology needed for implementing secure information sharing practices and in doing this from the perspective of the community of practice identifies where user practices are unable to support decision making needed for the successful operation of information security controls. As a result of this analysis, the constraints of staffing and other operational issues that would influence the implementation of both security practices and security technologies are also identified.

As can be seen, the capability maturity assessment approach contains techniques and methods that enable the development of an understanding of the community of practice that is affected by the system implementation so that designers can identify and understand the practices that individuals and groups need to adopt for a technology or practice to become integrated into daily practice [39, 40]. A community of practice approach is human-centred and places the communities into which the system is to be deployed and, not technology, as its starting point. It also centers on the practices that humans use to structure their relationships and working environment. This offers a potentially more culturally sympathetic starting-point than the technology-centred approach. The success of this approach has been demonstrated with the disemination of the this capability maturity assessment and improvement tool across the Australian primary healthcare sector [47].

This leads to the conclusion that communities of practice are more a function of social participation, where a created shared identity and engagement are derived through communal activity and experience (Wenger et. al 2004). The TIGS model therefore could offer a start-point for healthcare systems design which aligns better to front-line clinical practices and which is a process that would identify the clusters of practice related to information and its security, as part of the systems design process.

6 Conclusion

In both the UK and Australian cases there is a rhetoric of collaboration and even participation, however the approaches used do not appear to be true participation. The technical and management bias is a theme in both cases. Whilst from the perspective of Heek's framework it could be argued that these participative mechanisms sought to bring design and reality into contact, in practice the design always dominated reality and real engagement. In the Australian case, particularly the cursory perception is one of inclusion, yet in reality, particular groups dominated the design. It could be argued that a mistake of the UK EHR system design was to take a technology-centred view of information security issues and design requirements, and use the implementation of a technical system to force clinical process change. The results from broad, in depth reviews of the EHR programme, can be interpreted as describing a design-reality gap that left some clinicians with a security system that did not meet their needs and

which inhibited their clinical practice. This technically driven approach results in gaps in security practice and weakening of controls that can potentially affect patient safety.

There are many human-centred approaches to design but one that takes a community of practice focus is particularly relevant for information security. This results from focusing on the communities of practice as the unit of analysis enables the designer to understand information sharing and information access as a cultural phenomenon, and design the system accordingly. Without attention to the design-reality gap, there is a high risk of repeating the same mistakes. As the example of the TIGS model capability maturity assessment tool demonstrates, there are potential pathways to address these gaps at multiple levels. This paper acknowledges that whilst the initial design should be intrinsically supported by participative involvement to avoid and minimise the potential design-reality gap, the reality is that these gaps evidently exist. Where it is not possible to go back to re-design and start again, solutions to alleviate the impact of design-reality gaps have to be found.

The comparison of the security design aspects of the UK and Australian healthcare system development provided in this paper, and the subsequent application of a community of practice approach to security design in this context, provides a basis from which further security design methods can be explored.

Conflicts of Interest

The authors report no conflicts of interest.

References

1. Verizon. 2012 data breach investigations report (dbir) 2012. Available from: http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012-ebk_en_xg.pdf.

2. Hicks S. Russian hackers hold gold coast doctors to ransom (abc news). 2012 Available from: http://www.abc.net.au/news/2012-12-10/hackers-target-gold-coast-medical-centre/4418676.

3. Heeks R. Health information systems: Failure, success and improvisation. International Journal of Medical Informatics. 2006; 75(2): 125-37.

4. Greenhalgh T, Potts HWW, Wong G, Bark P, Swinglehurst D. Tensions and paradoxes in electronic patient record research: A systematic literature review using the meta-narrative method. Milbank Quarterly. 2009; 87(4): 729-88.

5. BBC. Nhs it scheme 'faces £600m cuts'. 2009 Available from: http://news.bbc.co.uk/1/hi/uk_politics/8400010.stm.

6. Department of Health. Dismantling the nhs national programme for it. 2011. Available from: http://mediacentre.dh.gov.uk/2011/09/22/dismantling-the-nhs-national-programme-for-it.

7. House of Commons Public Accounts Committee. The national programme for it in the nhs, The Stationary Office, Ed. 2007; House of Commons: London.

8. House of Commons Health Committee. The electronic patient record, sixth report of session 2006-2007, Office TS, Ed. 2007; House of Commons.

9. Rigby M, Budgen D, Turner M, Kotsiopoulos I, Brereton P, Keane J, Bennett K, Russell M, Layzell P, Zhu F. A data-gathering broker as a future-orientated approach to supporting epr users. International Journal of Medical Informatics. 2007; 76(2): 137-44.

10. Royal College of Nursing. Ehealth survey report. 2010. Available from: http://www.rcn.org.uk/__data/assets/pdf_file/0005/391109/004115.pdf.

11. Medix. Market research report: Rcn e-health study. 2007; Medix, UK.

12. Williams PAH. When trust defies common security sense. Health Informatics Journal. 2008; 14(3): 211-21.

13. Murray E, Burns J, May C, Finch T, O'Donnell C, Wallace P, Mair F. Why is it difficult to implement e-health initiatives? A qualitative study. Implementation Science. 2011; 6(1): 6-.

14. Turner W. Learning uk ehealth lessons: Dr justin whatling. eHealthspace 2012. Available from: http://ehealthspace.org/news/learning-uk-ehealth-lessons-dr-justin-whatling.

15. ISO. Iso/iec 27002:2005-information technology – security techniques – code of practice for information security management. 2005. Available from: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=50297

16. Pieters W, Coles-Kemp L. Reducing normative conflicts in information security. New Security Paradigms Workshop (NSPW 2011), Marin County, CA, USA, 2011.

17. Barman S. Writing information security policies. Indianapolis, Ind. : New Riders; 2002.

18. Parker D. Fighting computer crime. New York: Wiley; 1998.

19. Martin J, Frost P, O'Neill O. Organizational culture: Beyond struggles for intellectual dominance. Stanford Graduate School of Business Research Paper Series. 2004;(Technical Report 1864).

20. Beautement A, Sasse MA, Wonham M. The compliance budget: Managing security behaviour in organisations, in Proceedings of the 2008 workshop on New security paradigms. 2008; ACM: Lake Tahoe, California, USA. 47-58.

21. NEHTA. 2012 annual report: Connecting the circle of care. 2012. Available from: http://www.nehta.gov.au/.

22. NEHTA. Specifications and standards plan pcehr system version 1.4. 2011. Available from: http://www.nehta.gov.au/ehealth-implementation/pcehr-standards.

23. NEHTA. Nesaf r3.1 executive summary. 2012; (Version 3.1): 22. Available from: http://www.nehta.gov.au/connecting-australia/ehealth-information-security.

24. NEHTA. Nesaf r1.3 implementer blueprint. 2012. Available from: http://www.nehta.gov.au/connecting-australia/ehealth-information-security.

25. NHS. Information governance toolkit. 2000-2010 Available from: www.igt.connectingforhealth.nhs.uk.

26. NEHTA. Nesaf r1.3 business blueprint. 2012. Available from: http://www.nehta.gov.au/connecting-australia/ehealth-information-security.

27. Department of Health and Ageing. National e-health conference report. 2011. Available from: http://www.yourhealth.gov.au/internet/yourhealth/publishing.nsf/Content/nat-ehealth-conf-report/$File/eHealth%20Conference%20and%20Stakeholder%20Report.pdf.

28. Consumers Health Forum of Australia. Ehealth and electronic health records: Consumer perspectives and consumer engagement. 2010. Available from: https://www.chf.org.au/pdfs/rep/rep-651-eHealth-oct10.pdf

29. Akama Y. Politics makes strange bedfellows: Addressing the 'messy' power dynamics in design practice. In: Durling D, Rust C, Chen L-L, Ashton P, Friedman K, Eds. Undisciplined! Design Research Society Conference 2008, Sheffield Hallam University, Sheffield, UK: Sheffield Hallam University, 2009.

30. Baker B, Clark J, Hunter E, Currell R, Andrewes C, Edwards B, Vincent C. An investigation of the emergent professional issues experienced by nurses when working in an e-health environment. A collaborative project between the information in nursing forum at the royal college of nursing and school of health and social care, bournemouth university. Bournemouth University. 2007. Available from: http://eprints.bournemouth.ac.uk/11732/.

31. Eckert P. Communities of practice, in Encyclopedia of Language & Linguistics, Brown K, Ed. 2006; Elsevier Ltd. 683-5.

32. Wenger E. Communities of practice. A brief introduction. Communities of practice (c2007) Available from: http://www.ewenger.com/theory/.

33. Smith MK. Communities of practice. The encyclopedia of informal education 2003, 2009. Available from: http://www.infed.org/biblio/communities_of_practice.htm.

34. Lave J, Wenger E. Situated learning: Legitimate peripheral participation. Cambridge [England] Cambridge University Press; 1991.

35. Lesser EL, Storck J. Communities of practice and organizational performance. IBM Systems Journal. 2001; 40(4): 831-41.

36. Vitacca M, Mazzà M, Scalvini S. Socio-technical and organizational challenges to wider e-health implementation. Chronic Respiratory Disease. 2009; 6(2): 91-7.

37. MacFarlane A, Clerkin P, Murray E, Heaney DJ, Wakeling M, Pesola U-M, Waterworth EL, Larsen F, Makiniemi M, Winblad I. The e-health implementation toolkit: Qualitative evaluation across four european countries. Implementation Science. 2011; 6(1): 122-.

38. Murray E, Treweek S, Pope C, MacFarlane A, Ballini L, Dowrick C, Finch T, Kennedy A, Mair F, O'Donnell C, Ong BN, Rapley T, Rogers A, May C. Normalisation process theory: A framework for developing, evaluating and implementing complex interventions. BMC Medicine. 2010; 8(1): 63-.

39. May C, Finch T. Implementing, embedding, and integrating practices: An outline of normalization process theory. Sociology. 2009; 43(3): 535-54.

40. Murray E, Burns J, May C, Finch T, O'Donnell C, Wallace P, Mair F. Why is it difficult to implement e-health initiatives? A qualitative study. Implementation Science. 2011; 6(1): 6.

41. Tennant M. Psychology and adult learning. London: Routledge; 1997.

42. MacDonald K. Public hospitals uploading discharge summaries to PCEHR. Pulse+IT 2014; (22 January 2014). Available from: http://www.pulseitmagazine.com.au.

43. Tanenbaum, J., Tanenbaum, K., and Wakkary, R. Steampunk as design fiction. In: Proc. CHI'12, ACM. 2012; 1583-1592.

44. Vines, J., Clarke, R., Wright, P., McCarthy, J., Olivier, P., Configuring Participation: On How We Involve People in Design, In Proc. CHI'13. 2013

45. Sherwood, J; Clark, A; Lynas, D: Enterprise Security Architecture, A Business Driven Approach. 2005

46. Williams, P.A. H. (2007). Information Governance: A Model for Security in Medical Practice. Journal of Digital Forensics, Security and Law, 2(1), 54-67.

47. Royal Australian College of General Practitioners. (2013). Computer and Information Security Standards (Second Edition). Available from http://www.racgp.org.au/ehealth/ciss

Correspondence

Dr. Lizzie Coles-Kemp
Lizzie.Coles-Kemp@rhul.ac.uk

Associate Professor Trish Williams
trish.williams@ecu.edu.au