1-1-2012

Security Specialists are from Mars; Healthcare Practitioners are from Venus: The Case for a Community-of-Practice Approach to Security Architectures for Healthcare

Elizabeth Coles-Kemp
kemp@rhul.ac.uk

Patricia Williams
Edith Cowan University

Recommended Citation

Coles-Kemp, E., & Williams, P. (2012). Security Specialists are from Mars; Healthcare Practitioners are from Venus: The Case for a Community-of-Practice Approach to Security Architectures for Healthcare.
DOI: https://doi.org/10.4225/75/5795b34e3cf0e

DOI: 10.4225/75/5795b34e3cf0e
1st Australian eHealth Informatics and Security Conference, held on the 3rd-5th December, 2012 at Novotel Langley Hotel, Perth, Western Australia

SECURITY SPECIALISTS ARE FROM MARS; HEALTHCARE PRACTITIONERS ARE FROM VENUS: THE CASE FOR A COMMUNITY-OF-PRACTICE APPROACH TO SECURITY ARCHITECTURES FOR HEALTHCARE

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, Australia
[2]eHealth Research Group, Security Research Institute and School of Computer and Security Science,
Edith Cowan University, Australia
[1]lizzie.coles-kemp@rhul.ac.uk, [2]trish.williams@ecu.edu.au

Abstract
Information security is a necessary requirement of information sharing in the healthcare environment. Research shows that the application of security in this setting is sometimes subject to work-arounds where healthcare practitioners feel forced to incorporate practices that they have not had an input into and with which they have not engaged with. This can result in a sense of security practitioners and healthcare practitioners being culturally very different in their approach to information systems. As a result such practices do not constitute part of their community of practice nor their identity. In order to respond to this, systems designers typically deploy user-centred, participatory approaches to design using various forms of consultation and engagement in order to ensure that the needs of users are responded to within the design. Learning from international implementations of e-health, the development of the Australian electronic health records (EHR) system has been a participatory process. However, the more participatory approach has not been used as part of the technical security design of the e-health system and the functionality of the security governance architecture was not included in the process of consultation. Such exclusions result in a design-reality gap in so far as the healthcare systems as envisioned by designers are not easily related to by "front-line" clinical staff. Despite repeated design-reality issues in healthcare systems design, there is no fundamental change in the development paradigm to address the socio-technical security aspects of such systems. Indeed, the security perspective of system designers seems to originate from a very different perspective to that of front-line clinical staff. This discussion paper characterises the problem, uses examples from both the UK and Australian EHR experience, and proposes an alternative start-point to healthcare systems design.

Keywords
Information security, governance, electronic health records, e-health

INTRODUCTION

In 2010, significant parts of the UK's National Health Service IT Scheme were cut (BBC, 2009) and over the next 12 months the focus moved away from electronic healthcare systems that were designed and deployed from the centre to systems that allowed more choice at local level (Department of Health, 2011). Whilst the UK's National Programme for IT (NPfIT) was dismantled it left a number of successful EHR systems including: the 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. These are more than a collection of technical systems they are a combination of technical and human systems interwoven by working practices; a true socio-technical system. EHR is not simply the conversion of paper records to digitised records but offers the ability to "push the boundaries" of healthcare (Rigby et al., 2007) and transform the approach to the cycle of patient care. From a security perspective, the record can be used to document the health of the patient in any number of contexts and turns the record into a ubiquitous asset that takes many forms and is able to adjust its properties in response to the patient's care needs. The transformational nature of electronic health record (EHR) inevitably results in changes to clinical practices as well as data security practices. If the design of a socio-technical system such as EHR does not reflect how clinical staff perceive medical data and its role in patient care then practices may become disengaged and resistant rather than complementary and supportive practices. This disengagement can lead to work-arounds in the way information is handled. The UK's Royal College of Nursing have commissioned a series of surveys on the use of electronic health records since 2004 and whilst these surveys indicate that trust in the EHR systems have gradually increased, there was an initial feeling of systems being imposed on nurses. This response is supported by the findings presented in the House of Commons Select Committee reports.

Where system design is technology-centred rather than practice-centred, a gap often emerges which is filled by disengagement and resistance practices. This type of gap is characterised as the design-reality gap (Heeks, 2006) and has been identified as a common feature in healthcare system design. It leads to a form of resistance in the form of clinical work-arounds (Greenhalgh et al., 2009) in order to compensate for the lack of easy integration. A user-centred design approach seeks to reduce this gap by positioning the design from the perspective of the end-users of the system and by developing approaches which facilitate and enable dialogue between different stakeholders in the design process (Akama, 2009).

This paper argues that by focusing on the technical system, rather than the full socio-technical system, visceral aspects of information security are ignored and healthcare practitioners feel alienated resulting in resistance and disengagement in data security practices resulting from the design-reality gap. Furthermore, we argue that the methods used to develop overarching protection have alienated front-line clinical staff by presenting them with a picture of technology and of security that they do not relate to and thereby excluding them from the process of security integration.

This paper explores the issues and considers how a start-point of a community of practice approach to security design might help reduce the design-reality gap between security practitioners and clinical practitioners. The paper is composed thus: an illustration of the perception of the UK EHR system from the front-line, an evaluation of the information security management approach to the confidentiality, integrity and availability risks associated with the UK's EHR and those employed in Australia's e-health system, and design recommendations for a security management approach compatible with the consultative system's design approach found in Australia's e-health system development.

THE UK APPROACH

The UK's EHR system programme was subject to considerable public scrutiny. Numerous reviews were undertaken and subsequently reported. The 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 the perception "on the front line" was still one of imposition or a top-down system. In particular, the 2007 report from the committee 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.(House of Commons Committee of Public Accounts, 2006-2007).

The Committee's 2007 report goes onto 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 emphasizes the depth of the perception that the system was imposed top down and also illustrates a lack of confidence in those commissioning and managing the implementation of the system. This perception was derived from the UK's Royal College of Nursing which commissioned surveys since 2004 on their memberships' views and perceptions of EHR. (This paper focuses on the responses from the 2007 and 2010 surveys. In the 2010 the number of valid responses to the survey was 1308 and in 2007 this was 2,635). These surveys show that confidence in the system did increase between 2007 and 2010 and concerns about patient confidentiality slightly reduced. However, some of the qualitative interview answers appended to 2010 survey results also show that the perception of a gap between design and reality still existed for some clinical staff:

> 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…." (2010, p.27).

This response shows that, for this nurse, the process of design was technology-centred and in that setting this nurse found it difficult to articulate their feelings about technological change. This is an example of the types of feelings towards technology which often result in work-arounds and resistance.

In order for an EHR system to be successful, there must be a focus on understanding the system as the target user communities both see and relate to the system. A response in the 2010 survey illustrates the feeling that the target user community's requirements were not fully understood in the design process:

> 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…" (2010, p. 28)

Whilst the 2004 an 2007 surveys did not measure the perception of enforced system implementation and poor design, the qualitative responses to this effect were sufficient to be reflected in the Commons Select Committee report of 2007.

The design-reality gap was also discussed in the context of the security design aspects of the EHR. The Commons Committee report from 2007 indicates that security concerns were raised and highlighted as part of the review process. The quote below clearly illustrates that whilst for some clinicians technical and human systems go hand in hand when responding to concerns of an information security nature, the Department of Health foregrounded the technical 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.[82] 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." (2007, p. 21)

When considering the UK's EHR system it is important to consider not just the technical system but also the organisational aspects. An EHR is a socio-technical system containing the technical system, governance system and working practices. Security is integral to how healthcare information is used and shared. It has long been recognised that successful information security management approaches are ones in which all members of the organisation are engaged (ISO, 2005). 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 participatory (Pieters & Coles-Kemp, 2011). In organisational literature these cultures are often referred to as a strong unified culture. Examples of this implicit approach can be found in numerous information security management writings on policy design (Barman, 2002; Parker, 1998). 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" (Martin et al., 2004 p. 8). This process of reinforcement is typically part of the process of embedding information security policies within an organisational unit. The intention is not necessarily one of enforcement; the intention is often that the organisation and its units will adapt the governance approach to fit their organisation. However, compliance processes result in organisations and its units being adapted to fit the governance structure (Beautement et al, 2008).

When designing the EHR system, the National Health Service (NHS) also designed a governance framework underpinned by the following organisational aims (NHS, 2000-2010):

1. Support the provision of high quality care by promoting the effective and appropriate use of information
2. Encourage responsible staff to work closely together, preventing duplication of effort and enabling efficient use of resources
3. Develop support arrangements and provide staff with appropriate tools and support to enable them to discharge their responsibilities to consistently high standards
4. Enable organisations to understand their own performance and manage improvement in a systematic and effective way

The NHS information security framework is based on ISO 27001 and latterly its healthcare derivative, ISO 27799. In order to support working practices, the NHS produced a template model and toolkit for managing information governance according to the type of healthcare organisation. Examples of healthcare organisations include Acute Hospital Trust, Ambulance Trust, General Practice, Mental Health Trust and Social Care. The toolkit focuses on information and its control, and considers the control of information from the perspective of the systems containing the information. The toolkit contains the following requirements:

- Specification of requirements (depending on organisation type)
- Assessment criteria
- Guidance documents
- Access to a helpdesk

The intention is that health organisations adopt the templates and then apply them using the information security management guidance provided.

This security management approach is a further example of a centrally designed framework that can be interpreted as a top-down approach towards information security and preserves the design-reality gap because the governance practices do not reflect or align with the working practices of clinical staff. It is an approach that emphasises how culturally different security and healthcare practitioners are.

The results of the design-reality gap can be seen in the reports of the Commons Selection Committee from 2007 and 2010, and ultimately in the decision in 2010 to move away from centrally designed systems to systems that better reflect the requirements of the local health organisation. Arguably, had a user-centred design approach been used which included elements of participatory and co-design (Akama, 2009), the design-reality gap might have been reduced and a system more compatible with the front-line clinicians' requirements produced. In particular, this approach might have produced a design that more accurately reflects the requirements related to healthcare information access. However, a user-centred approach is not the only requirement. It is clear from the reports that it was the information and technology start-point itself that was problematic as well as the systems design approach used. The start-point of information and technology is one that alienated some clinical staff from relating to the EHR systems produced.

THE AUSTRALIAN APPROACH

In comparison, the development of Australia's new e-health system has employed a participatory approach to the technology and architecture design with the use of tiger teams, community consultation and clinical lead engagement (NEHTA, 2011). Where a "Tiger Team is a group of experts assigned to investigate and/or solve technical or systemic problems" (NEHTA, 2011). Indeed the use of such teams was designed to speed up the process of development of the standards required and 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 a user participation involvement. The tiger teams involved in the security governance framework and the health summary record (known as the personally controlled electronic health records (PCEHR)) security risk assessment only involved those with security expertise and did not include clinical staff. Therefore it takes the view that security is a technical specialism and not a system dimension that can be designed by non-technical specialists.

Whilst the Australian response shows engagement of technical expertise for security functional design with less clinical workflow input, thus the perspective is still culturally more technology-centred (NEHTA, 2012) and there was still little engagement on aspects of management or governance and working practices. Whilst the overall approach in Australia has increased stakeholder consultation (Department of Health and Aging, 2011) the security design aspects of the initiative were still approached in a technology-centred using subject matter experts and did not incorporate engagement by front-line clinical practitioners. Indeed, whilst there were some 450 stakeholders engaged, 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 (Department of Health and Aging, 2011). This raises the concern that whilst system design engagement of this type aims to be broad and inclusive, it was in the Australian case 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 (2011) "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, it 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 focusing on the consumer control (privacy and controlled access) and resulted in the opt-in system (Consumers Health Forum of Australia, 2010). Such an approach is not a fully participatory practice as design is still driven by the interests of one stakeholder group over another. It is also an approach which has as its start-point, information and systems and not the practices of the clinical practitioners. 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. The result is an EHR that prioritises one set of stakeholder requirements over another.

COMMUNITY OF PRACTICE: AN ALTERNATIVE START-POINT

Research has demonstrated that in the healthcare environment the strong top down approach causes a strategic gap in the appropriate engagement with the new ehealth, and associated management systems (Baker et al., 2007). This is an example of the design-reality gap (Heeks 2006). This is in part attributed to the perception of devolved accountability from management to front line healthcare staff who have had less input as stakeholders to the systems they are expected to adopt and use. As a result the systems are technology and information-centred, and do not necessarily align with the healthcare practice goals of frontline clinical staff. In particular, systems that are focused on specific information goals do not easily support information sharing and access requirements that occur within the networks of clinical practice. These are the networks that develop within a work place and demonstrate the design-reality gap. Likewise, an information security governance framework that is information-centred rather than healthcare practice-centred, equally conflicts with the networks of clinical practice.

Networks of practice are often referred to as "communities of practice" and offer an interesting alternative start-point to healthcare systems design. Eckert (2006) 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 good information security practice. Wenger (c2007) defined communities of practice as "Communities of practice are 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 (Smith, 2003, 2009; Lave and Wenger, 1991). Hence, the proposition is that community of practice learning, and subsequently change, is derived from social experience (Lesser and Storck, 2001). Lave and Wenger refer to this as 'situated learning'. Extrapolating this to learning and 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 (Eckert, 2006). Indeed since communities of practice materialize from engagement in common goals or interests they are fundamental to the participation and perception of the environment in which they operate.

A Community of Practice Approach to Security Architecture Design

An approach to system access design based on central criteria, assessment criteria, guidance documents and access to a help desk places information rather than working practices and relationships at its core. Given the design-reality gap that follows, it could be argued that this is the wrong start-point and reflects the cultural differences between systems and security practitioners, and clinical practitioners. It is clear that this start-point, of centralising information access requirements, is at odds with the way in which clinical staff carry out their day to day work. An alternative view is that "The real technology is the human resource available to hospitals, homes and social health organizations" (Vitacca, Mazzù, & Scalvini, 2009). Hence, a framework is needed to explore and interpret how this human technology can interoperate with EHR systems. One sociological approach is a theoretical framework to support and interpret the interplay of technology and social activity developed using 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 (MacFarlane et al., 2011). NPT addresses the gap between research and application, and focuses on "implementation and integration of interventions into routine work (normalisation)" (Murray et al., 2010). This work reflects a community of practice approach to understand the practices that individuals and groups need to adopt for a technology or practice to become integrated into daily practice (May & Finch, 2009; Murray et al, 2011). A community of practice approach is human-centred and uses the human, 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 systems starting-point than the technology-centred approach.

In order to operationalise such an approach within design, it is important to consider how a community of practice needs to be supported. Wenger (c2007) suggests that to support a community of practice you need to recognize the domain (the identity of the shared commitment and competancy of the group); the community (the relationships that the domain members possess); and the practice (the shared resources, expereinces and ways of ddealing 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 de-contextualized, abstract or general (Tennant 1997). This results in a shared co-participation in socially based integrated with cognitive processes,

and this develop socio-cultural practices specific to that community. As such it also affects those coming in and out of the community and as well as those that interface with it, otherwise known as peripheral participation.

This leads to the conclusion that communities of practice are more a function of social participation, where a created shared identity and engagement is derived through communal activity and experience (Wenger et. al 2004). This therefore could offer a start-point for healthcare systems design which is aligned 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.

CONCLUSION

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. This mistake resulted in a design-reality gap that left clinicians with a security system that did not meet their needs and which inhibited their clinical practices. The usual response to this type of gap is to talk about "bottom-up" system design. However, as the Australian design programme shows, this can still result in design-reality gaps. Whilst Australia has studied how other countries has approached the development of their national e-health system and adjusted their approach in light of the lessons learned, Australia may be at risk of repeating the same mistakes in relation to the underpinnings and security foundations of these systems.

Perhaps, therefore, more fundamentally the design focus needs to shift from a technology-centred to a human and practice-centred focus. One such human and practice-centred approach is one based on communities of practice. As a conceptual perspective of instilling a security culture and facilitating sound adoption of security management practices, whilst also developing a long-term organisational memory, a community of practice approach is a means to this end. Fundamental to the effectual utility of such healthcare communities of practice, is the inclusion and immersion of the healthcare participants in the information security function. Future work in this area will consider how this issue can be rectified. It will use international case studies for comparison, and consider the design principles for a community of practice approach to information security management and governance. This is important in order to anticipate what a community of practice driven approach to participatory design would look like, and what governance framework to accommodate this might be developed.

REFERENCES

Akama, Y., (2009) Politics makes strange bedfellows: addressing the 'messy' power dynamics in design practice, *Undisciplined! Design Research Society Conference 2008, Sheffield Hallam University, Sheffield, UK, 16-19 July 2008*

Baker, B., Clark, J. D., Hunter, E., Currell, R., Andrews, C., Edwards, B. D. & Vincent, C. (2007). *An investigation of the emergent professional issues experienced by nurses when working in an e-health environment.* Bournemouth: School of Health and Social Care, Bournemouth University.

BBC. (2009). NHS IT scheme 'faces £600m cuts'. Retrieved from http://news.bbc.co.uk/1/hi/uk_politics/8400010.stm

Barman, S. (2002). *Writing Information Security Policies*. New Riders: Indianapolis, Ind.

Beautement, A., Sasse, M.A., & Wonham, M. (2008). The compliance budget: Managing security behaviour in organisations. In *Proceedings of the 2008 Workshop on New Security Paradigms*. ACM, Lake Tahoe, California, USA. 47-58.

Consumers Health Forum of Australia. (2010). *eHealth and Electronic Health Records: Consumer Perspectives and Consumer Engagement*. Retrieved from https://www.chf.org.au/pdfs/rep/rep-651-eHealth-oct10.pdf

Department of Health. (2011). Dismantling the NHS National Programme for IT. Retrieved from http://mediacentre.dh.gov.uk/2011/09/22/dismantling-the-nhs-national-programme-for-it

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

Eckert, P. (2006). Communities of practice. *Encyclopaedia of language and linguistics.*

Greenhalgh,T., Potts,H., Wong,G., Bark,P., & Swinglehurst,D. (2009) Tensions and Paradoxes in Electronic Patient Record Research: A Systematic Literature Review Using the Meta-narrative Method. *Milbank Quarterly. 87*(4) 729-788

Heeks, R. (2006). Health Information Systems: Failure, Success and Improvisation - *International Journal of Medical Informatics, 75*, 125-137.

House of Commons Public Accounts Committee (2007). *The National Programme for IT in the NHS*. HC 390. London. The Stationary Office.

ISO. (2005). *ISO/IEC 27002:2005-Information technology -- Security techniques -- Code of practice for information security management.* Retrieved from http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=50297.

Lave, J. & Wenger, E. (1991). *Situated learning: Legitimate peripheral participation*. Cambridge: Cambridge University Press.

Lesser, E. L. & Storck, J. (2001). Communities of practice and organizational performance. *IBM Systems Journal, 40*.

MacFarlane, A., Clerkin, P., Murray, E., Heaney, D., Wakeling, M., Pesola, U.-M. & Winblad, I. (2011). The e-health implementation toolkit: qualitative evaluation across four European countries. *Implementation Science, 6*(1), 122.

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

May, C., & Finch, T. (2009). Implementation, embedding, and integration: an outline of Normalization Process Theory.. *Sociology, 43*(3), 535 - 554.

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

Murray, E., Treweek, S., Pope, C., MacFarlane, A., Ballini, L., Dowrick, C., et al. (2010). Normalisation process theory: a framework for developing, evaluating and implementing complex interventions. *BMC Medicine, 8*(1), 63.

Parker, D.(1998). *Fighting Computer Crime*. Wiley: New York.

NEHTA. (2011). *Specifications and Standards Plan PCEHR System Version 1.4*. Retrieved from http://www.nehta.gov.au/ehealth-implementation/pcehr-standards

NEHTA. (2012). *NESAF R1.3 Business Blueprint*. Retrieved from http://www.nehta.gov.au/connecting-australia/ehealth-information-security

NHS. (2000-2010). Information Governance Toolkit. Retrieved from www.igt.connectingforhealth.nhs.uk

Pieters, W., and Coles-Kemp, L (2011). Reducing normative conflicts in information security. *New Security Paradigms Workshop*.

Rigby, M., Budgen,D., Turner, M., Kotsiopoulos, I., Brereton, P., Keane, J., Bennett, K., Russell, M., Layzell, P. & Zhu,Adata, F. (2007). Gathering broker as a future-oriented approach to supporting EPR users, *International Journal of Medical Informatics 76* (2-3):137–144.

Smith, M. K. (2003, 2009). Communities of practice. *The encyclopedia of informal education*. Retrieved from www.infed.org/biblio/communities_of_practice.htm.

Tennant, M. (1997). *Psychology and Adult Learning*. London, Routledge.

Vitacca, M., Mazzù, M., & Scalvini, S. (2009). Socio-technical and organizational challenges to wider e-Health implementation. *Chronic Respiratory Disease, 6*(2), 91-97.

Wenger, E. (1998). *Communities of Practice: Learning, Meaning, and Identity*. Cambridge, Cambridge University Press.