MEDINFO 2010
C. Safran et al. (Eds.)
IOS Press, 2010

doi:10.3233/978-1-60750-588-4-228

Clinicians, security and information technology support services in practice settings- A pilot study

Juanita Fernando

Mobile Health Research Group, Medicine Nursing and Health Sciences, Monash University, Melbourne, Australia

Abstract

This case study of 9 information technology (IT) support staff in 3 Australian (Victoria) public hospitals juxtaposes their experiences at the user-level of eHealth security in the Natural Hospital Environment with that previously reported by 26 medical, nursing and allied healthcare clinicians. IT support responsibilities comprised the entire hospital, of which clinician eHealth security needs were only part. IT staff believed their support tasks were often fragmented while work responsibilities were hampered by resources shortages. They perceived clinicians as an ongoing security risk to private health information. By comparison clinicians believed IT staff would not adequately support the private and secure application of eHealth for patient care. Preliminary data analysis suggests the tension between these cohorts manifests as an eHealth environment where silos of clinical work are disconnected from silos of IT support work. The discipline-based silos hamper health privacy outcomes. Privacy and security policies, especially those influencing the audit process, will benefit by further research of this phenomenon.

Keywords:

Health information, Medical informatics, Information protection, Data security, Hospital information system, Privacy, eHealth, Sociotechnology**.**

Introduction

This paper analyses feedback from information technology (IT) support staff and clinicians about their perceptions of work with eHealth security implementations in the natural hospital environment (NHE). Key features of the NHE include inadequate infrastructure, pervasive computer use, shared clinical workspace, aural privacy shortcomings, highly interruptive work settings that threaten private and secure (P&S) e-health training outcomes and inadequate budgets [1].

Studies reviewing clinician work with P&S eHealth tools in the NHE began emerging from the 1980s. For the purposes of this paper, the term *eHealth* broadly refers to patient health records stored on computers in care settings. Theorists recognized the potential synergies between clinical work and IT support [2-4]. The studies are among the forerunners of multidisciplinary knowledge about the impact of IT support on clinical work with eHealth. Sociotechnical approaches advance our current understanding of eHealth implementations too [4-9]. Sociotechnical approaches "consider and optimize both the technical work processes and the social systems operating within the work environment to improve organizational performance" [7]. Post and Kagan's (2007) study of security tools trade-offs to maintain productivity furnishes an example of the sociotechnical approach in action [9].

The 2008 study by van der Linden et *al.* reviews P&S issues in the context of interoperable systems architecture emphasizing the need for a paradigm shift from centralised to localised systems to advance P&S patient care[10]. Other important works, such the efforts of Brogan et *al.* (2007), in the context of password security tools, and Williams (2008), who analysed P&S tools in the GP setting, try to understand the end-user experience of eHealth implementations [11,12]. Notably, Pagliari (2007) maintains the common pattern of working in discipline-based silos has supported the development of an IT environment that runs in parallel, rather than harmoniously, with the clinical user environment [2]. The literature suggests understanding the P&S interface between clinicians and IT support staff is a foundation of improving eHealth performance in patient care settings [5]. Hence this pilot work analyses beliefs of IT staff about work with P&S in an eHealth hospital context and contrasts this with the findings from an earlier case study of clinicians in the NHE [1].

Method

IT participants were drawn from a purposive sample of IT staff at public hospitals in Victoria (Australia). "*IT staff*" refers to hospital staff with reporting lines to executive information managers. The participants were recruited from tertiary hospitals in rural, urban and suburban locations. After human ethics clearance, managers passed on recruitment material for the study during regular meetings with groups of staff. Nine IT staff from various departments, as is illustrated in "Table 1. IT participant profile" volunteered to join the study.

Table 1- IT Participant profile

Area	Case	Sex	Title
Urban	1	M	IT Manager
	2	M	IT Manager
Subur-ban	3	M	Clinical Informatics Manager
	4	M	Computer Services Manager
	5	M	Departmental IT Officer
	6	M	Departmental IT Support Officer
Rural	7	F	Health Informatics Services Manager
	8	F	Hospital IT Support
	9	M	Hospital IT Manager

Case study data from the second group of participants, clinicians, has been added to IT data and is re-used for this work. The clinical participants comprised nine medical, eight nursing and nine allied health participants. That study asked about clinician security practices when using health systems for patient care. The participants were drawn from various departments of the same hospitals as IT participants [13]

The sampling and ethics methods for the older work reflected those used for this case study. A lack of available volunteers meant no attempt was made to select participants based on specific clinical or IT disciplines. The data collection factor in common was that all participants worked with P&S eHealth tools for patient care at the Victorian public hospitals. Presumably participants that volunteered for these studies were more interested in P&S than their counterparts.

Both case studies relied on the 'questerview' technique, which asks standardized questions during qualitative data collection [13]. Participant questions were structured, ostensibly to obtain closed answers during interviews, which were tape recorded by the researcher for later qualitative analysis. The juxtaposition of clinician feedback, published earlier, with the new data from IT support staff at the same hospitals compliments our present understanding of work with P&S in eHealth settings.

Results

The results section initially aggregates key feedback from the clinicians. A report of feedback from the IT participants follows. Taken together, the sections summarize all of the key research data underpinning this work.

Clinical evidence

Key clinician feedback is depicted in "Table 2. Summary of the clinicians' evidence" [13]. As the table shows, clinicians were required to share computers at the user-level environment. Queues for access to the computers were frustrating and delayed patient care tasks so that clinicians "sometimes did not bother" updating patient records on eHealth systems at all.

The system environment for eHealth was described as 'sluggish' by participants. Software evidently did not intercommunicate, even when on the same computer. Most applications required a unique logon combination of user-name and password for access to care information enabling clinician access to a single episode of patient care. Computerised access control lists, which tailored an individual's authorisation to eHealth systems by patient consent and work role, were characterized as cumbersome and ineffective. Finally screen-savers asking for a logon combination to continue work interrupted the diagnostic process as well as costing valuable time for patient care. Screensavers blank a monitor when no user activity has been sensed for a period of time. Feedback suggested the system environment was so slow and cumbersome; it often disrupted patient care work.

Table 2- Summary of the clinicians' evidence [14]

Implementation	Manifestation	Result
Shared computers	Queue	Frustration
Slow system	System latency	Disruptive
eHealth applications	Multiple logons	Impractical
Passwords	Fear of lockout	Avoidance
"Handover sheets"	Paper persistence	Collusion
PKI	Inflexible	Collusion
IT Support	Authority	Resignation

Passwords for logon to the eHealth system were also too numerous for participants. One medical clinician explained the range of passwords he needed to remember exceeded one's cognitive capacity. Forced password resets and alphanumeric, mixed-case combinations (e.g. M0n@5h) to enable ostensibly safe user choices exacerbated the shortcomings participants associated with the P&S tool. Further, the clinicians felt the process of obtaining a replacement password, should one be forgotten, was both tedious and frustrating. Fear of system lockout as a consequence of forgetting passwords triggered a range of clinician responses, from the illicit storage of the combination on a computer screen or notice board, to "cheat sheets" in some settings, generic ward logons and avoidance techniques, such as sharing logons. These shared logons often gave greater access to the eHealth system than the clinicians own and so were seen as pragmatic solutions for access to patient care information at all system-levels.

The table also illustrates the clinicians' beliefs that "*handover sheets*", as the clinicians called them, were an "important medical tool*"*. The sheets amalgamate patient information from a range of eHealth systems into a printed document. Sharing user credentials with colleagues allowed written updates from ward rounds to be transcribed by a staff member later in the day. Collusion over eHealth P&S tools for access to productive patient information from "the multiplicity of systems on wards" was a common participant experience.

Public Key Infrastructure (PKI) was apparently inflexible for use in patient care settings. PKI protocols incorporate digital signatures and digital certificates, which are protected by passwords or keys, to decipher encrypted data. The protocol relies on evidence of identity, generally a face-to-face check, conducted by the issuing authority [14]. Several clinicians evinced concern about the effectiveness of the security tool. For instance, PKI authenticates users for eHealth. However if the authenticated clinician leaves the computer without logging out then others might harness the PKI authorisation

for their own purposes. Given the highly interruptive NHE, this scenario often occurred in patient care settings at the hospitals. In some cases the collusion was deliberate, with clinicians often sharing their PKI user details with others during holidays or illness. In other cases, the interruptive nature of clinical work underpinned the breach. The clinicians' believed PKI was no more robust than any other security tool used in patient care settings and, in any case, would increase their dependence on IT departments.

The participants believed IT departments at the hospitals were responsible for most eHealth shortcomings. They were worried by system failure at the hospitals, although could not quantify its frequency. The expression "IT failure" was used to describe all the technical difficulties the clinicians had ever experienced or heard of in the NHE. Preparing for IT failure, one participant backed up her own system storing "paper copies of pretty much everything" on her computer. A staff survey expressing dissatisfaction with clinical IT devices were the substance of a complaint from another but "nothing …happened". Other clinicians believed IT departments "really don't meet the times [sic]". Most clinicians had "simply given up" on IT support because "the process was too much of a hassle".

Evidence from IT staff

This section reports on key data collected for this study about supporting secure clinical work with eHealth. Key themes from interviews with IT staff are summarized in "Table 3. Summary of the IT support feedback". The table illustrates IT staff feedback about personnel and technical resources shortages linked to inadequate budgets. The following comment from one participant epitomises these. He said, "No we can't afford that" in reference to a P&S tool. Another participant explained, "We're only a small team", referring to her department. Still another said, **"**We are so small …I think everywhere bogs in these days … you have to, haven't got much choice". Finally, a fourth IT participant suggested resources shortages meant IT staff were not always trained for the tasks they did. He said, **"**I haven't got teams of specialist people, they're all multi skilled … one of my colleagues did an upgrade yesterday … half past five last night we're ringing him up to find out certain things because the documentation was incomplete". Participants believed IT resources were inadequate to support their hospital communities efficiently.

As Table 3 illustrates, the IT support staff also thought maintaining a secure eHealth clinical setting was demanding. The participants knew their responses were being recorded while talking about clinicians as end-users, yet were very frank throughout questerview. One participant explained, "[eHealth P&S] is very challenging, you've got to drum it into … [users]". Yet another IT participant said "one of the things we've got to do is get security into … [users] … People don't realise that an instant could be all it takes for somebody to try and enter the computer". All IT staff had noticed clinicians using stick-it notes and cheat sheets to store username and logon combinations in patient care settings. Still another IT worker wryly commented "we will tell the business manager the password and they will give it to … [others]". A tangible frustration with the clinicians' priorities permeated the feedback. Yet participants were also resigned to managing eHealth P&S risks in clinical settings. The relationship between IT and the clinicians was sometimes contradictory.

Table 3- Summary of the IT support feedback

Experience	Manifestation	Result
Shortages	Small teams	Technically inefficient
Clinicians	Incomprehension	Resignation
Password administration	P&S tools escalate	Counterpro-ductive
CD, DVD, USB	Locked down	Flash cards
Support structure	Fragmented	Disconnection
Auditor	P&S reports	Key priority

The table also lists passwords as a key P&S concern for IT. All the participants helped to administer "one end-user one logon combination" policies at the hospitals. However complaints from clinical departments sometimes caused policy adaptations such as generic user names (i.e. "Ward 21"), where many clinicians shared a single computer account. One IT participant, summing up her colleagues feedback said, "[In] … certain wards, it's a balancing act between the [P&S implementations and clinicians' patient care work]". Evidently IT work included making pragmatic judgements about the quality of P&S tools for care in the NHE.

Notably, the IT participants, as with the clinicians, spoke about the range of logon combinations required for complete access to a single patient care record. One IT participant explained, "… you only need one username and password for both [hospital] systems. However for security you have to set up an[other] account." Evidence from the IT staff suggests P&S system requirements multiplied the number of logons need for clinician access to eHealth systems.

For the most part IT staff reported locking down Universal Serial Bus (USB) ports and portable media at the hospitals. The USB ports enable portable devices to connect to a computer without restarting it. However other staff explained this was not always the case. One participant said, "every Tom, Dick and Harry uses their USB to take [data] home". It seems even after locking down USB ports and CD or DVD drives at the hospital where he worked "Flash memories come in [sic] and people just walk in and out with the bloody stuff". Flash memories are electronic cards that store data. The feedback suggests that as security controls were implemented at the hospitals, clinicians found ways to avoid them.

Several participants commented on the structure of IT support services at the hospitals. One IT participant explained support responsibilities were fragmented. He said "what I am doing is not complete by itself, for many things I go back to [other IT staff]." He continued "… for any change, there is a Change Manager, we have to go through him personally". Another participant confirmed the feedback. Speaking about requests for IT support, he explained, "you could fix [the job] there and then but there's a procedure … part of that is the security, its

only a subsection of it [sic].” The participant was then called away to organise a major system change, ending the questerview. The reported segregation of many duties apparently ensured IT participants tended to be time-poor and disconnected from each other.

Finally, as Table 3 suggests audit priorities were paramount for the NHE. Feedback indicated IT policies were audited by external health authorities every few years to renew hospital licences. Annual internal audits of the hospitals were outsourced to contractors. The frequency of both types of audit depended upon previous findings.

Most IT participants spoke about policies emerging from audit requirements. The policies forced many of the password practices that the clinicians found cumbersome. These policies included the multitude of numbers required to authenticate eHealth access, forced password resets and alphanumeric password selection. One IT participant described the audit process. He said “… as part of a review, we have to look at everything … we have to present all our documentation to the auditors”. A participant from another hospital agreed. She said “Yes … [the auditors] … come in and interfere sometimes, well … strongly suggest that you adopt, with financial incentives or otherwise with disincentives [sic] [their preferred P&S systems]. The feedback implies that auditors generally relied on paper-based or electronic reports to inform their findings and recommendations. IT Support participants, for seemingly pragmatic reasons, considered audit requirements a higher priority than clinician P&S support tasks in the NHE.

Discussion

Three key themes emerged from this comparison of clinician feedback with that of IT staff at the hospitals. The themes concern eHealth resources, the functionality of several P&S tools and evidence of tension between both groups of participants.

Resources

Comments made by both clinician and IT participants illustrate the point made by Post and Kagan (2007), who argue organisations rarely deliver the increased IT support required to adequately underpin P&S implementations[10]. IT resource constraints, such as an inadequate number of computers and associated access queues, eHealth applications that didn’t interoperate and multiple logons for a coherent view of patient information frustrated the clinicians. As a result, some clinicians did not always update patient care records.

IT participants consistently referred to shortages of technical resources and skilled staff. These participants explained the IT teams were, by necessity, multi-skilled in a practical sense if not by certification. IT teams were time-poor due to their small size and the breadth of their responsibilities in the NHE.

The combined experiences of both cohorts are worrisome. The feedback suggests care information stored on eHealth systems may not be reliable for patient care. Auditors provided financial incentives to decide on P&S policies. The time-poor IT teams comprised a resource shared by clinicians, as well as other sections of hospital communities at the sites. The consequence of these experiences may be three-fold. Firstly, eHealth systems are likely to hold unreliable data. Secondly, unreliable data can foster adverse health affects (AHEs) for patients. Finally, the P&S tools utilized for access to eHealth were not tailored to contextual clinical needs. These findings suggest health authorities should review access to resources in the NHE to address the P&S issues emerging from questerview evidence.

Usability

The evidence indicates that clinicians did not find the eHealth system usable. “*Usability”* is a term describing the ease with which users can interact with a computer system. The clinicians believed the system was slow, clumsy and ineffective, or even worse, interrupted the diagnostic process. Applications on the same computer frequently could not communicate with each other let alone networked computers. The participants believed P&S tools for eHealth, such as logon combinations, were both onerous and numerous.

The clinicians’ widespread fear of system lockout due to forgetting one’s password resulted in the eHealth avoidance techniques, as Post & Kagan suggest [10]. The questerview evidence suggests these techniques included the illicit storage and publication of logon combinations, collusion over user credentials and the use of handover sheets, which were based on transcribed data, to provide patient care. Transcribed notes have long been associated with mistakes that cause AHEs[14]. The clinicians saw no point in PKI implementations in care settings due to their interruptive work flow. Frustrated by disruptive eHealth tools, the clinicians tended to believe IT services were at least partly responsible for their lack of control over the storage of patient care information.

Audit

IT staff feedback suggests many eHealth P&S tools made the clinicians’ concerns difficult to address. Hospital eHealth systems did not require multiple logons but P&S controls did. The P&S controls were required to pass regular system audits underpinning hospital licenses.

It seems audits, some contracted internally, generally reviewed eHealth P&S policy documentation and system processes. IT participants explained audit reviews did not extend to actual user environments. Local audits were evidently triggered by actual security incidents occurring between the hospital audits. Once effective controls to the local threat had been developed, they were incorporated into policy documents for the next audit.

The external audit process has much to commend it. The process addressed conflict of interest concerns at the hospitals. Also, system concerns were incrementally controlled as they arose and were looped back into hospital policy for future audits. Yet feedback from both groups of participants suggests a gap in the crisis management audit approach – the patient care setting. The feedback shows clinicians habitually addressed their own eHealth concerns in isolation from IT. It is reasonable to assume this habit resulted in relatively few

crises, limited IT support, and so solutions were rarely incorporated into hospital audit policies. As a consequence, unless thoroughly reviewed, audit processes may prove irrelevant to numbers of AHEs or threats to the P&S of eHealth systems.

Tension

The relationship between IT staff and clinicians was tense. The evidence indicates the clinicians believed eHealth systems were unreliable and controlled their access to patient care information. P&S trade-offs, such as shared passwords, allowed the clinicians to avoid using eHealth systems and so minimised the need for IT support. The cohorts evinced frustration with each other throughout the questerviews.

IT support staff believed achieving P&S eHealth systems in end-user environments was challenging. For instance directives to lock down removable media, such as USB ports, were corrupted by end-users carrying flash memory cards. Logon combinations were commonly stored on stick-it notes and displayed at the hospitals too. The IT staff felt they needed to "drum" P&S eHealth practices into the clinicians.

A clear contradiction between clinician and the IT work goals emerged from questerview evidence. IT tools disrupted patient care work, potentially fostering AHEs. So these were often thwarted by clinicians at the hospitals. The IT staff were both frustrated by clinicians and, by contrast, were also resigned to clinician P&S practices. Evidence suggests the participants were locked into disciplinary silos.

These findings support Pagliari's (2007) reflection about parallel clinician and IT work practices [2]. Participants did not acknowledge their differing motives and operational constraints. Thus the contribution of further research trying to understand or develop active collaboration between clinicians and IT support will advance P&S concerns. The collaborations may also reduce the number of AHEs associated with poor eHealth implementations.

Conclusion

This work compares the approach of IT support staff and with that of clinical staff to eHealth as it relates to the P&S of patient care data to show that neither cohort felt they could control P&S at the hospitals. Their evidence suggests resources shortages combined with clinician avoidance of eHealth manifested as tension between both cohorts of health workers. Further research is needed to understand the undoubted impact of resource shortages, usability and tension between IT and clinicians on effective eHealth implementations.

Acknowledgment

I am grateful to the reviewers for their contribution to this paper.

References

[1] Fernando J, Dawson L. The health information system security threat lifecycle: An informatics theory. Int J Med Inform. 2009;78(12).

[2] Pagliari C. Design and evaluation in eHealth: Challenges and implications for an interdisciplinary field. J Med Internet Res. 2007 April - June 2007;9(2):e15.

[3] Shortliffe EH. Sem-Plenary: The evolution of health-care records in the era of the Internet. MedInfo; 1998; Seoul; 1998.

[4] Hannan TJ. The Regenstrief Medical record system: A quarter century experience. Int J Am Med Inform Assoc. 1999;54(3):225-53.

[5] Weingart P, ed. Interdisciplinarity: the paradoxical discourse. Toronto, ON: University of Toronto Press 2000.

[6] Kaplan B, Shaw N. Future directions in evaluation research: people, organizational, and social issues. Methods Inf Med. 2004;43(3):215-31.

[7] Westbrook JI, Braithwaite J, Georgiou A, Ampt A, Creswick N, Coiera E, Iedema R. Multimethod evaluation of information and communication technologies in health in the context of wicked problems and sociotechnical theory. JAMIA. 2007 Nov 1, 2007;14(6):746-55.

[8] Harrison MI, Koppel R, Bar-Lev S. Unintended consequences of information technologies in health care: An interactive sociotechnical analysis. JAMIA. 2007 Sept 1, 2007;14(5):542-9.

[9] Post GV, Kagan A. Evaluating information security tradeoffs: Restricting access can interfere with user tasks. Computers & Security. 2007;26(3):229-37.

[10] van der Linden H, Kalra D, Hasman A, Talmon J. Inter-organizational future proofEHR systems A review of the security and privacy related issues. Int J Med Inform. 2008 Aug 27;78(3):141-60.

[11] Williams P. When trust defies common security sense. Health Informatics J. 2008;14(3):211-21.

[12] Brogan M, Lin C, Pai R, Kalet I. Implementing a mandatory password change policy at an academic medical institution. In: AMIA, editor. AMIA Annu Symp Proc; 2007 Oct 11; 2007. p. 884.

[13] Fernando J. An analysis of current clinician security practices while using health information systems security in Australian public hospitals. Melbourne: PhD thesis, Monash University 2008:330.

[14] Gutman P. PKI: It's not dead, just resting. Computer. 2002;35:41-9.

Address for correspondence

Dr Juanita Fernando
Monash University Clayton 3800 AUSTRALIA
Telephone +61 3 9905 8537 Facsimile +61 3 9905 9327
Email: juanita.fernando@med.monash.edu.au