Abstract

Enthusiasts of eHealth implementations for use in clinical care settings claim axiomatic privacy and security (P&S) outcomes. Evidently, “eHealth” has acquired meaning for the enthusiasts when, as with Jabberwocky, the claims seem to make their own sense. Yet emerging work suggests the claim may be nonsensical. The openEHR and other international endeavours have advanced efforts to overcome the technical mismatch between clinical settings and much eHealth, so enabling technically secure tools. However an understanding of the actual work context is needed to fully appreciate the factors that influence P&S in eHealth. Thus, this work analyses clinician critiques of eHealth experiences in relation to the Jabberwocky to support an understanding of P&S in care contexts. Twenty-three medical, nursing and allied health clinicians working in Australia (Victoria) participated in this qualitative study examining work practices with P&S for patient care.

Participants criticised slow, inefficient eHealth information systems permeated by usability errors. EHealth applications expanded workloads and system demands were onerous, increasing the clinicians’ scepticism of reliance on information technology. Consequently many clinicians had developed trade-offs to avoid reliance on them. The trade-offs include IT support avoidance and shared passwords to PKI and computer accounts. Handover sheets populated by transcribed notes were circulated between clinicians. The practices ensure paper persistence and escalate threats to data confidentiality, integrity and availability. Study evidence suggests claims about P&S tools that are inherent to eHealth applications are nonsensical, foster unintended consequences, hamper patient care and represent a larger P&S threat than indicated by most studies to date.

1. Introduction

A search of emerging publications in the eHealth systems domain tends to locate manuscripts exploring the clinical adoption of new and emerging eHealth innovations. Much work claims the eHealth innovations enhance privacy and security (P&S) by supporting data confidentiality, data integrity and data availability (data-CIA). Data confidentiality refers to access that is tailored by authorisation. Data integrity is data that is reliable and up-to-date. Data availability refers to information that is accessible whenever and wherever it is needed. Many of the publications suggest data-CIA is axiomatic in the context of eHealth applications and associated tools by potentially reducing the need for costly health budgets and eliminating data fragmentation to improve patient care outcomes [1-2].

Other work has increasingly linked unintended adverse patient-safety consequences to the innovations [3-5]. The findings from many emerging peer reviewed publications emphasise a growing concern about the quality of patient eHealth care outcomes and the way these may be affected by data-CIA threats. This is explored more fully throughout this work.

2. The literature

Few peer-reviewed publications in the literature are founded on research explorations looking to understand the actual, as opposed to the perceived, clinician eHealth P&S experience, although there are some notable exceptions such as Koppel et al. [3] or Westbrook et al. As Greenhalgh et al. (2009) point out many assertions about data-CIA in patient care settings are supported by a relatively narrow body of literature and are restricted to largely experimental or quantitative research designs [2]. Patient care settings tend to comprise outdated infrastructure, pervasive computer use, shared clinical workspace, aural privacy shortcomings, interruptive work settings, confusing legislative frameworks, poor privacy and security (P&S) eHealth training outcomes and inadequate budgets [1]. Real-life patient care settings configured with eHealth tools remain largely unexplored.

Interactions between eHealth innovations, health organisational settings and the clinical team are complex. Recent research suggests the clinical team is one of the most important environments at which information is communicated and patient care work is negotiated [1, 7, 8-9]. Evidently human intervention will always be required in patient care settings regardless of eHealth innovation [7, 16].

A number of international proposals for developing integrated and standards-based eHealth have been underway for some time. They include:

- the OMG (Object Management Group)/CORBAmed (Common Object Request Architecture) service interface definitions
• HL7 (Heath Level 7), a messaging and EHR proposal
• the CEN (Comité Européen de Normalisation) and
• OpenEHR (Electronic Health Record) proposals [9].

Standards are “documents, established by consensus and approved by a recognized body, that provide, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context” [10]. Dialogue looking at the composition of EHRs has converged and intensified over recent years, with international endeavours analysing messaging, communication, data standards and codes and contributing valuable material to the discussion, informing standards development achievements accordingly.

Groups such as openEHR routinely involve practising clinicians, considered domain experts, into their international endeavours. OpenEHR is founded on the concept of archetypes. An archetype is a “re-usable formal model of a domain concept”[11]. Archetypes are partly designed to allow experts, such as clinicians, to create data definitions that will inform their eHealth systems in care settings. The concepts include elements such as diagnosis, microbiology results and weight and are designed to be future-proof regardless of IT platform [11]. The convergence between openEHR, other standards-based groups and clinicians show promise for the future of eHealth tools.

Combined with open interfaces between the clinicians and health informaticians, emerging publications are also beginning to yield new knowledge about eHealth. However the specific P&S risks caused by threats to data-CIA in the patient care setting are usually overlooked in these publications [3, 12-13]. We wonder whether eHealth P&S tools are Jabberwocky-like in real life contexts, only making sense to eHealth enthusiasts while considered nonsense by clinicians providing patient care. “Jabberwocky” is a poem of nonsense verse that makes sense internally and is written by Lewis Carroll for the children’s book “Through the Looking Glass” [14]. This paper addresses real-life data-CIA oversights by reporting actual user-level perceptions of eHealth P&S tools in care settings.

3. Method

We used the qualitative case study method for this research, which explores clinician perceptions of their eHealth information system P&S experiences in care settings. The study relied on the ‘questerview’ technique to gather participant feedback during interviews. ‘Questerviews’ apply standardised questions and questionnaires during qualitative data collection, combining qualitative and quantitative research methods.

4. Discussion

4.1. Workspace environment

Shared offices and computers are a notable feature of clinical work in the user-level environment. Six of twenty-six participants always shared office space with colleagues. Another twelve clinicians functioned in private offices, though many patient care tasks took place in workgroup offices or on hospital wards. Finally, eight clinicians provided
patient care in private office spaces or on the wards. All of the clinicians shared computers and workspace for at least part of the time they were engaged in work with eHealth to provide patient care.

The clinicians explained shared office space resulted in the regular display of sensitive health information to individuals that were not directly involved in a patient’s “chain of care”. There was “lots of patient care information” on the participants’ “open desk” in shared workspace. Participants also commented they often lined “… up at the computer” to work with patient information in shared clinical workspaces, which logically suggests data was displayed to others in the queue and passers-by regardless of clinician intent to protect P&S. As is illustrated in “Table 1: Workgroup environment: A cross case effects matrix”, the clinicians believed P&S shortcomings linked to shared workspace and PCs meant data-CIA was “impossible!” to achieve.

| Table 1. Workspace environment: A cross case effects matrix |
|-----------------|-----------------|-----------------|
| Context         | Functionality   | Effect          |
| Shared office and workgroup PC | Routine patient information displays | Impossible to achieve private environment |
| No aural privacy | Medical record not always updated | Pertinent questions not always asked of patients |
| No physical privacy |                      | Frustration |
|                  |                      | Avoidance of security tools |

The Table also sums up feedback suggesting the clinicians believed achieving aural privacy was “untenable” in the shared workspace. They routinely overheard the content of telephone conversations about colleagues’ patients while going about their everyday work and one participant speculated that others in the workgroup, from another discipline, also understood the content of her phone conversations about patients (“... and they're [colleagues] overhearing what's happening and vice versa”). Evidently, individuals within earshot of health information exchanges were not always involved in a patient’s “chain of care”.

The table also summarizes participant comments about aural privacy, which could not be achieved at the patient bedside or within the nurse station on wards. Participants explained the station was “too noisy, [and] there are too many people around that can overhear [sic]”. Conversations held within curtains at the patient bedside were also audible to nearby individuals. One participant commented “…when we see patients [in their beds], it’s terrible because they've got "the magic curtain", as we call it, no-one can hear … (laughter)”. Another referred to eavesdroppers on the ward - “…you know "bed 23" next door is listening in to every word “.

Aural privacy shortcomings meant, as Georgiou, Westbrook and Braithwaite et al. point out [6], that participants sometimes did not ask relevant questions during bedside consultations, “even the question we need to [sic]”. Other participants altered their clinical communication style (“I'm conscious of what I say … and who's listening”). As one participant facetiously suggested, the only way clinicians could ensure aural privacy was to use “sign language”.

Aural privacy in shared clinical workspace was so poor that many participants were expected to, and had, autonomously adopted a range of gatekeeper strategies to control the security shortcoming. These strategies resulted in “whispered consultations [held] in the passageway”. One clinician explained that she was always “… conscious of … who’s listening” to the conversations. Another clinician believed aural privacy was about colleagues “… trying to be responsible”. Logically then, aural privacy concerns at the hospitals were likely to threaten the confidentiality of sensitive patient information and the partial information that often results from the data-CIA threat may jeopardize future health care outcomes.

Queues for access to shared computers were customary on the ward and in workgroup offices. One clinician explained the arrangements complimented existing hospital infrastructure. She said, “… you just physically can't have an office for every clinician … not where you've got group workstations.” Many participants commented they often lined “… up at the computer” to work with patient information.” As Table 1 illustrates, the queues frustrated clinicians and delayed patient care tasks.

| Table 2. System environment: A cross case effects matrix |
|-----------------|-----------------|-----------------|
| Context         | Functionality   | Effect          |
| Computers & associated P&S tools | Slow | Data not available when and where needed. |
| Screen savers   | Productivity costs | Interruptive |
| Access control lists | Clinician anger | Not usable |

4.2. System environment

Participants were universally critical of the system resources they depended on for information in care settings. The slow and inefficient or, as one clinician described them “sluggish”, eHealth systems shaped the P&S of patient care. Many systems were unable to intercommunicate, even when located on the same computer. The communication shortcomings cost inordinate amounts of clinician time.

Some participants believed the slow and inefficient systems reflected business decisions taken at senior levels of the hospitals. One clinician attributed the speed problem to version conflict issues. Apparently, as “Table 2: System environment: A cross case
effects matrix” indicates, eHealth systems were slow because clinical software was outmoded and various iterations of the same software were utilized throughout the hospitals (“we've got different systems, Kestral for us ... different Kestrel for [other departments], HOMER... [for still another department]”). The iterations were not interoperable.

Most participants maintained the processing speed of computer technology was inadequate for routine work with an eHealth system. Feedback revealed logon processes took large blocks of time (“...the current system has a very slow logon”). Apparently, slow logons were worsened by the number of personnel on a computer network (“Every log on... takes about two to three minutes... [and depends on] how many people are logged on for the [computer] network”.

Slow eHealth systems meant some participants needed to wait a couple of minutes before acquiring clinically productive information. It was time consuming to obtain a patient’s record for theatre or other medical treatment and “…it [took] ...forever to logon to the computer... ...inordinate amounts of time [were] ...taken getting access to information ...[there was] a lot of delay ...[the process was] a pain in the arse [sic].”

Clinical frustration with the queues noted earlier was aggravated by logging on and off shared computers featuring access control lists (ACL) for every application (“you've got to be jumping between systems or screens and closing on and off and that kind of thing”). Clinicians needed to “check three or four different places” to establish access to information. They commonly spoke about the “…large ... time issue” involved in checking an ACL in their “busy workplace”.

Interoperability shortcomings exacerbated the productivity cost of establishing access to patient information, with one participant mentioning individuals “who were literally red with rage” about the privacy enhancing implementation. Evidence from the user level environment suggests ACL may underpin the confidence health authorities have in eHISs at the hospitals, but ultimately usability shortcomings, reinforced by their productivity cost and the antipathy of many clinicians to their implementation, may undermine the efficacy of ACLs to secure patient health data.

A small group of participants suggested patient records were not always updated with pertinent information as a result of their frustration with security tools on shared computers (“...sometimes we don’t bother [to update electronic records]”). The frustration was exacerbated by queues for computer access. Avoidance of updating records on eHealth systems hampered data integrity and availability, cornerstones of medical error [1].

Screensavers at the hospitals generally required a password or keystroke to dismiss. A screensaver is a program that blanks out a monitor display if no user activity has been sensed for a period of time [1]. Study findings were divided according to the relationship between system demands and the productivity cost of each type of screensaver in a clinical setting. That is, clinical productivity outcomes shaped participant beliefs about screensaver implementations.

It seems some screensavers interrupted the diagnostic process, forcing clinicians to re-enter logon combinations periodically during patient care (“It becomes a real mine [field] trying to manage the thought processes which are going on”). Clinical work was forced to centre on ongoing system demands rather than health care outcomes (“It ... annoys the doctors because they go away and do a procedure and then come back to dictate and ... the screensaver's on ...”).

One participant reported the security screensaver frequently “shut down” wireless computers. The clinician was so frustrated by the implementation that he had deactivated his screensaver “… for its ... ethics”. He felt the screensaver did not take contextual circumstances into account so he removed it. Thus, the evidence indicates some screensavers impeded clinical productivity and so were avoided.

Inefficient eHealth systems at the hospitals aggravated participant concerns about screensavers. Feedback indicated sluggish systems lengthened the time period before a clinician could return to work with a record (“I have to wait for [the logon prompt] ... to click up, I have to wait for it to go through a little exit thing and whatever, so it can take couple of minutes before I can even get access to anything”). Hence, affected clinicians believed the system demands that were associated with most screensavers were “unworkable”.

By contrast, screensavers requiring a keystroke to dismiss made relatively minor system demands in patient care settings. Clinicians were happy to work with these because the security tool “really [didn’t] ... affect patient care work ... at all.” Study findings suggest that screensavers requiring a logon to dismiss were far less usable than their counterparts in clinical settings at the hospitals.

### 4.3. Passwords

<table>
<thead>
<tr>
<th>Context</th>
<th>Functionality</th>
<th>Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security tool designed to support a tailored and secure view of the patient record Computers &amp; associated P&amp;S tools</td>
<td>Too many</td>
<td>Fear of lockout</td>
</tr>
<tr>
<td></td>
<td>Not useable</td>
<td>Supports data availability</td>
</tr>
<tr>
<td></td>
<td>Displayed close-by eDevice</td>
<td>Passwords shared to avoid impeding patient care</td>
</tr>
<tr>
<td></td>
<td>Shared logons</td>
<td>Pragmatic access to patient care information</td>
</tr>
</tbody>
</table>
Secure passwords are often complex to remember and can make it difficult for authorized end-users to access a system [1]. Feedback about password-based logon implementations in care settings garnered intense participant criticism. Fear of system lockout due to the implementations saturated “questerview” feedback. The implementations potentially barred participant access to an eHealth system, conceivably interfering with a key foundation of improved patient care. A summary of the feedback is illustrated in “Table 3: Passwords: A cross case effects matrix”.

The range of passwords required to obtain access to complete patient records on eHealth systems meant “[… you really have to go through a lot of passwords to get [patient care] … information]” and each application required a unique password (“I have so many …”). The number of passwords clinicians needed to remember for patient care was worse for those who practiced at more than one hospital (“… each hospital will have a different password”). One participant described the passwords as an “impost” and believed between the hospitals and one’s personal life, password system demands were “beyond a joke!”

Participants could not rely on memory for password access to an eHealth system because, including private lives, the average number of secure passwords each clinician needed to remember (often dozens of them) exceeded the cognitive capacity of most humans [9]. While a few clinicians explained password selection was a routine matter, many of them found it “a pain”. The application of random elements for secure password selection, such as alphanumeric characters (e.g. M0n@$h1 for monash1), amplified participant criticism. One participant commented “having a mixture …” of characters made passwords so “… difficult to remember” she had to note them somewhere … “defeating …the whole purpose of passwords”. The study indicated that unless written down, password controlled security tools conceivably locked participants out of eHealth systems applications.

Forced password resets “every few weeks” aggravated participants’ woes. One participant explained she scrolled through numbers to renew a password, adding a “one, two, three, four” and so on each time. She believed as “We’re all very predictable people” that most of her colleagues utilised the same strategy. Yet the more predictable a password is, the easier it is to discover, threatening information breaches [18]. Therefore, while predictable passwords may threaten P&S, the range and complexity of passwords clinicians needed to remember for patient care work meant predictable passwords were also usable passwords.

What is more, clinicians who hadn’t accessed a particular eHealth systems in four to six weeks were evidently locked out of eHealth systems thereafter (“The passwords cut out …so often if you haven’t used it and you go to open [an eHealth record] … your password’s gone again”). Clinicians then required IT support with regard to a new password, adding further productivity delays. Thus, participants felt password processes wrested control over information supporting patient care away from clinicians. Many of the participants explained that patient care work did not involve ongoing clerical struggles with eHealth systems. Password sharing practices were an acceptable and a pragmatic response to perceived shortcomings with eHealth security tools. Consequently, password sharing was a customary clinician practice at the hospitals.

Passwords were illicitly stored and disseminated across all hospital sites. Written passwords were frequently attached to computer monitors (“… the logon combinations are stuck on the left side of the computer”) and others were listed on ‘cheat sheets’ (“They have a cheat sheet in some places”). Yet other passwords apparently ended up on information displays (“[passwords] end up on a list on a wall” [gestures to example]).

The evidence was reinforced by feedback indicating several participants customarily got “somebody else” to logon to an eHealth system, which one clinician referred to as the “big monster”. Another participant commented that recently, a colleague “either didn’t do the work that she was supposed to do on eHealth systems because she couldn’t get in, or was constantly trying to trace somebody else to log her on.” Alternatively, when clinicians were absent, passwords were provided to colleagues over the phone (“… they will ring me and I will tell them the password …”). Participants rostered onto shift work ‘borrowed’ the accounts of colleagues so security screensavers would not activate during the night (“can you log into this computer for me so it doesn’t go off in the middle of the night?”). Others shared screensaver passwords to expedite clinical productivity (“I’m trying to do five things at once and typing and sometimes I’m the only person there. … it can be difficult so people get around it by using other people’s passwords and logging in”). Finally, still other participants reported utilizing single, department-wide, passwords because they believed individual logons would take “too long” to utilize in patient care settings. Thus, the evidence suggests participants routinely traded-off the security of unique and individual passwords. The trade-offs facilitated unobstructed clinical access to private patient information stored on eHealth systems throughout practice settings, thereby enhancing participant control over the security tool and clinical productivity.

Along with shared workgroup resources and workspace, comments about slow and inefficient computer systems and security tools emerged throughout data collection. Screensavers and ACLs were impractical to use in care settings. The range of passwords required for access to eHealth systems exceeded human cognition so passwords were illicitly stored or shared. The systems were not useful and meant interactions between clinicians and computers were onerous and, if possible, avoided.
4.4. Handover

Although studies have shown some handovers involve verbal reporting during morning meetings or over coffee, most ad hoc procedures at the hospitals meant clinicians generally carried handover sheets with them throughout a shift [15]. As the feedback in “Table 4: Handover: A cross case effects matrix” suggests, handover sheets were an “important medical tool”, amalgamating patient information from a range of eHealth systems into a single document. Thus, participants avoided the need to use security tools for access to “the multiplicity of systems on wards” to obtain productive patient information.

Notably, updating the handover sheets may have involved collusion with unqualified personnel. As with other studies, Timmons’ UK data indicates collusion over unique passwords does occur in clinical settings, despite the threat of legal sanction [17]. This probably happens because, as the US work by Lending & Dillon argues, many clinicians do not comprehend the importance of eHealth system P&S [18]. Training shortcomings meant clinicians did not believe an eHealth system was any more or less confidential than a paper record [9]. It is evidently as clinically acceptable to share passwords with colleagues, as it is to share clinical workspace or computer accounts.

Participants made notes on the handover sheets during patient care and most seemed to put these onto the computer later. Sometimes handwritten notes were transcribed back into an eHealth system by non-medical personnel, such as ward clerks. While difficult to estimate the extent of password sharing, it was reported by a substantial number of clinicians, across all hospitals, during ‘questerview’. Ergo, most participants circulated handover sheets, for later transcription by oneself or a colleague, to all clinicians on a shift during the provision of patient care.

Handover sheets enabled participants to provide patient care according to “their own kind of little system”. The sheets could be tailored to personal style, which was seen as positive. The evidence showed clinicians at the hospitals believed the sheets provided a more reliable and productive source of patient care information than an eHealth system. However data detailed on the sheet were a partial snapshot of patient health, limited to a single clinician’s personal notes taken during the current work shift and based on transcribed records. Patient information was integrated and transcribed on a computer template at the end of each shift. Although constantly and immediately available regardless of location, transcribed handover sheet templates risked perpetuating data fragmentation on eHealth systems. Errors mistakenly transcribed into an eHealth systems template potentially provide the basis for future, updated, sheets and so on, in an ongoing error loop. Thus, handover templates suggested a clinical association between paper persistence and clinical productivity resulting in medical error at the hospitals.

Evidently most handover sheets were disposed of in an appropriate “confidential storage bin” at the end of each work shift. However it seems “many have turned up in supermarkets”. Several participants explained that the Health information can “float around” on a ward or were left “lying around” for “anybody to read”. One participant found handover sheets useful to take home to file “a record of what happened on a shift”. While the sheets were generally destroyed in accordance with hospital security policies, evidently this was not always so. Thus, eHealth systems contained usability errors, facilitating collusion over passwords and other

<table>
<thead>
<tr>
<th>Context</th>
<th>Functionality</th>
<th>Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ongoing transcription template</td>
<td>Saves time</td>
<td>Supports data availability</td>
</tr>
<tr>
<td></td>
<td>eHealth system not auditable</td>
<td>Clinician control of patient care information</td>
</tr>
<tr>
<td></td>
<td>Errors in transcription</td>
<td>Supports mobility</td>
</tr>
<tr>
<td></td>
<td>May be retained by clinician</td>
<td>Pragmatic collusion</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Paper persistence</td>
</tr>
</tbody>
</table>

The sheets were carried by all case study participants during patient care, with “60 plus” printed and circulated to “all the staff”. The handover sheet meant clinicians did not need to queue for access to a workgroup computer to obtain patient information each time it was required. The consequence of the queues, as shown above, was that not all patient records were updated with pertinent patient information. The handover sheets meant it did not take “inordinate amounts of time” to access the information due to delays caused by sluggish computer applications and ACLs. In particular, one participant pointed out obtaining patient records from a range of computer applications was “not really” a clinical “skill” and “such a waste of time” and felt she needed “a secretary” to manage the job.

The subject of handover sheets was evident throughout ‘questerview’ feedback. Participants reacted in an ostensibly logical and pragmatic fashion to eHealth systems that were not usable by trading them off for the constant, immediate and mobile availability of handover sheets. The sheets, which were based on transcribed patient care notes, are a potential cause of data fragmentation and medical error [1, 4]. Nonetheless, paper records, such as handover sheets, sustain communication between clinicians to support patient care practice [16]. The sheets are a contextual means of ensuring clinical productivity in eHealth environments at the hospitals.
workarounds to ensure clinician control over security tools. This meant patient information stored on handover sheets was vulnerable to error as well as other P&S breaches.

4.5. PKI

Participants believed Public Key Infrastructure (PKI) frameworks promoted data fragmentation in clinical settings. Yet Australian health authorities have nominated it as their preferred authentication framework [20]. At the time of data collection, the clinicians had limited experience of PKI since it was not widely used to share patient information over the Internet. Nonetheless several clinicians demonstrated a good appreciation of the technology. Therefore their feedback, as summarized in “Table 5: PKI: A cross case effects matrix”, was incorporated into data analysis for this study.

Several participants understood the co-dependent relationship between PKI and the physical P&S measures that protect access to clinical computers. Once PKI was installed on a computer, clinicians had to ensure one “…didn’t leave your computer and give somebody else access to [an encrypted] file or [digital] signature”. Yet earlier feedback (in the context of workgroup resources) demonstrated the participants did tend to leave screens open and share computer accounts.

| Table 5. PKI: A cross case effects matrix |
|---|---|---|
| Context | Functionality | Effect |
| Robust security tool | Co - dependent on physical security | Hinders clinical productivity |
| | Relies on mutual trust | Clinicians claim no need, so avoid |
| | | Trust system reinforced |
| Handover sheets | Shared logon information | Trust system entrenched & passed on to recruits |
| Transcription | Night shift support | Data breach customary although often confined to the care setting |
| | Mobile patient record | |

While working with patient information in the highly interruptive clinical milieu, it seems participants were regularly called on for help and so sometimes forgot to log out of computers. Frequently, this was not consciously done. The interruptions, combined with shared clinical workspaces and devices, ensured participants could not control the physical P&S of patient care at the hospitals. Co-dependent PKI technology was not effective at the user-level environment and the shortcomings, which promoted data fragmentation and information breach, meant it was unlikely the allegedly robust technology was much more secure than any other P&S implementation at the hospitals.

4.6 Trust

Lending and Dillon’s study, as pointed out earlier, argues the nurse clinicians they surveyed did not comprehend the importance of eHealth system P&S in clinical settings [18]. One clinician interviewed for this research commented that she did not “know of any cases of identity fraud …” These beliefs, shared by the majority of clinicians, may be due to an emphasis on trust in user-level clinical settings. A small number of participants believed clinicians may “rely a bit too much on expecting [other] people … to have the same [P&S standards]” as they did. Several other participants, speaking about phone passwords and secure fax processes, mentioned their signature or identity was never validated by other health service organisations (“no one ever verifies [who I am]”). Further, “Unless a recipient return[ed] a fax, you actually did not know it had been sent to a wrong number”. Ergo, as one participant explained: “In the end the [health] system works on trust, whatever bits and pieces you've got in the place.”

| Table 6. Trust: A cross case effects matrix |
|---|---|---|
| Context | Functionality | Effect |
| Collusion | | Trust system entrenched & passed on to recruits |
| Handover sheets | Shared logon information | |
| Transcription | Night shift support | Data breach customary although often confined to the care setting |

Some participants believed trust was sufficient security protection for information, as shown in “Table 6: Trust: A cross case effects matrix” above. It seems PKI exceeded the P&S needs of patient information on eHealth systems (“I don’t know if [PKI] would be that useful… don’t see a great need for that level of security”). The belief that trust was a more effective security implementation than PKI technology was surprising.

The clinical value system, viewed in the context of work looking at individualism versus collectivism, might be characterized by cultures of logic and trust respectively. Hofstede & Hofstede argue that in some cultures, commonly held value systems maintain collective interests should prevail over individual interests, based on notions of reciprocal trust” [21]. Clinicians are also influenced by the notion of *primum non nocere*, or “do no harm” [1] and may assume all clinicians are inherently trustworthy since the philosophy underpins clinical training across the globe. Perhaps participant lack of control over P&S tools at the hospitals meant the clinicians believed trust cultures were a secure and more effective clinical productivity measure than inflexible PKI? An examination of trust-based health cultures warrants a more thorough investigation than this work can provide although indicates the importance of further research across the sector. In short, study findings suggest participants relied on trust cultures to control the P&S of patient.
information stored within user level environments at the hospitals rather than inflexible and co-dependent information security tools and frameworks.

4.7. The IT department

Organizations rarely deliver the increased IT support required to adequately underpin P&S implementations [1, 13]. As “Table 7: IT departments: A cross case effects matrix” shows, participants, in the context of feedback about eHealth security tools, tended to concur. Several clinicians attributed usability shortcomings to IT departments.

Notably, technicians working in IT departments did not generate the same level of trust as other hospital colleagues, or ‘insiders’. Some insiders were possibly more equal than others or IT personnel may have been considered ‘outsiders’ because their practice is not directly controlled by the everyday patient care. In any event, study findings show the clinicians tended to circumvent personnel employed by hospital IT departments, not to mention avoiding the IT system itself.

Participants considered system failure to be a large risk associated with eHealth, though unable to quantify the frequency of IT downtime. The expression “IT failure” seemed to be a catch all term describing most technical difficulties clinicians had experienced at the hospitals. In preparation for IT failure, one participant backed up her own system storing “paper copies of pretty much everything” on her computer, which included sensitive patient health information. Another argued, regardless of “…when the IT system [was] …down, patient information remained accessible on a handover sheet” rather than on an eHealth system. Many participants considered hospital IT systems too uncontrollable to rely on for constant and immediate clinical access to patient care information.

Clinician perceptions of PKI were coloured by more general scepticism about the IT department. Participants were concerned the “extra layer of complexity” PKI adds to eHealth systems (see earlier). They believed this would increase dependence on the department. Once installed on a computer, clinical productivity “would depend how good your IT department” was, “It would depend on the PKI program” and how IT departments configured clinical computers. Participant views about PKI usability shortcomings were apparently linked to perceptions of IT departments.

Password utilisation was also affected by clinician perceptions of IT departments. It seems the process of obtaining a new password was long and convoluted. The vast majority of participants spoke of frustration when dependent on the IT departments for password access to eHealth systems, justifying their reliance on handover sheets and entrenching data fragmentation through paper persistence. Many clinicians had “simply given up” on IT support because “the process was too much of a hassle”.

Some participant views were probably influenced by a limited understanding of IT in clinical workspaces. Many clinicians were not computer literate and were scared of eHealth security tools, which they could not understand or control. Several participants indicated ongoing and contextual training was required before eHealth would become a useful part of work practice.

Findings from a survey expressing dissatisfaction with the usability of clinical IT devices were the substance of a complaint to IT at one hospital. However when clinicians asked the IT department to provide further training, “nothing …happened”. Other participants believed IT departments “really don’t meet the times [sic]”. In short the clinicians believed IT departments could not or would not adequately support their control of eHealth PaS implementations at the hospitals.

5. Conclusion

International organisations, such as openEHR and CEN, are trying to work more closely with practising clinicians. This dialogue may result in the development of usable and standards-based eHealth systems. However the results of these efforts have not trickled down to effect the experiences of the clinicians participating in this work.

This work analyses clinical perceptions of seven key themes and the resulting effect on the P&S of patient care information. Shared workspaces and resources combined with slow systems and unwieldy tools, such as the range of user logons needed to ensure a coherent view of patient records, supported by trade-offs such as transcribed handover sheets,
mutual trust, and universal participant antipathy towards IT, characterise eHealth system security at the user-level environment. The perceptions influence the reliability and validity of patient health information stored on eHealth systems in the care context.

Study findings suggest control of clinical productivity, possibly due to the perception that high quality patient care outcomes were hampered by P&S tools, was the over arching concern of the time-poor participants. Enthusiastic claims as to the utility of eHealth in clinical settings were considered Jabberwocky-like, nonsense, countering attempts to deliver efficient and effective patient care. Thus, poorly configured eHealth systems jeopardised the P&S of sensitive patient care health information, not to mention actual improved patient care outcomes.

7. Acknowledgements

Jennifer Lindley, Academic Advisor MBBS Curriculum, Faculty Medicine, Nursing & Health Sciences, Monash University, Monash, Australia “Brain-stormer par excellence.”

6. References


