International Journal of Medical Informatics xxx (2015) xxx–xxx

Contents lists available at ScienceDirect

International Journal of Medical Informatics

journal homepage: www.ijmijournal.com

Designing for privacy management in hospitals: Understanding the gap between user activities and IT staff's understandings

Elizabeth V. Eikey (B.S.)[a], Alison R. Murphy (B.S.)[a], Madhu C. Reddy (Ph.D.)[b,*], Heng Xu (Ph.D.)[a]

[a] College of Information Sciences and Technology, The Pennsylvania State University, USA
[b] Department of Communication Studies, Northwestern University, USA

ARTICLE INFO

Article history:
Received 12 January 2015
Received in revised form
11 September 2015
Accepted 25 September 2015
Available online xxx

Keywords:
IT Staff
Workarounds
Collaboration
Privacy
Electronic health record (EHR)
Users

ABSTRACT

Purpose: We examined the role of privacy in collaborative clinical work and how it is understood by hospital IT staff. The purpose of our study was to identify the gaps between hospital IT staff members' perceptions of how electronic health record (EHR) users' protect the privacy of patient information and how users actually protect patients' private information in their daily collaborative activities. Since the IT staff play an important role in implementing and maintaining the EHR, any gaps that exist between the IT staff's perceptions of user work practices and the users' actual work practices can result in a number of problems in the configuration, implementation, or customization of the EHR, which can lead to collaboration challenges, interrupted workflow, and privacy breaches.
Methods: We used qualitative data collection methods for this study. We conducted semi-structured interviews with 20 hospital IT staff members. We also conducted observations of EHR users in the in-patient units of the same hospital.
Results: We identified gaps in IT staff's understandings of users' work activities, especially in regards to privacy-compromising workarounds that are used by users and why they are used.
Discussion: We discuss the reasons why this gap may exist between IT staff and users and ways to improve IT staff's understanding of why users perform certain privacy-compromising workarounds.
Conclusion: A hospital's IT staff face a daunting task in ensuring users' collaborative work practices are supported by the system while providing effective privacy mechanisms. In order to achieve both goals, the IT staff must have a clear understanding of their users' practices. However, as this study highlights, there may be a mismatch between the IT staff's understandings of how users protect patient privacy and how users actually protect privacy.

1. Introduction

Privacy and collaboration are two central concepts in healthcare. Patient-care teams must continuously share confidential information about patients in order to do their work. However, there are often tradeoffs between sharing patient information to deliver quality and timely healthcare and protecting the patient's information. Health information technologies (HIT), such as the electronic health record (EHR), are meant to facilitate medical employees' collaborative work practices while maintaining mandated levels of patient privacy protection. Protecting patient privacy includes ensuring the confidentiality, integrity, and security of patient data, as well as ensuring the appropriate use and distribution of patient data [1]. Many EHR systems are designed in a one-size-fits-all fashion by vendors, whose primary privacy focus is on developing security features that meet regulatory and legal requirements. Consequently, information technology (IT) staff in hospitals are faced with the challenge of configuring and customizing these generalized EHR systems so that they adequately support the workflows of hospital staff while still providing effective privacy protection mechanisms [2].

The EHR's privacy protection mechanisms include access control mechanisms (e.g., unique user login, strong passwords) [3–6], automatic time-out, audit trails [7,8], and data encryption [9,10]. While these mechanisms are important to ensure the privacy of patient data, they can also negatively impact collaboration [5,6,11]. For example, Heckle and Lutters [6] found that the single login to

* Corresponding author at: Department of Communication Studies, School of Communication, Northwestern University, Evanston, IL 60208, USA.
E-mail address: mreddy@northwestern.edu (M.C. Reddy).

http://dx.doi.org/10.1016/j.ijmedinf.2015.09.006
1386-5056/

EHR systems was effective in administrative areas of the hospital but it had adverse effects on collaboration for clinical staff. Especially in areas where there are high collaborative needs, such as in the emergency department (ED), role-based access along with single login presents a number of issues. Because of role-based access, users can have different system rights that may prevent them from being able to see all of a patient's record or restrict them from being able to add or update patient information in the system. Additionally, the clinical staff are frequently moving throughout the hospital when taking care of patients, which requires them to continuously log in and log off from the EHR (due to timeouts, user change, walking away from the screen, etc.). The constant interruption required to log in and log off can negatively impact clinical staff's ability to effectively work together [6,11]. Additionally, users having to remember passwords for various systems can also create collaborative issues. For instance, in one situation, two nurses were required to collaborate on approving a patient's medication. However, in order for the second nurse to review and confirm the medication administration, she had to remember a password that she rarely used [6]. Therefore, EHR privacy mechanisms can be in conflict with the collaborative nature of hospital work and lead to user frustration and challenges during collaborative patient-care activities.

The IT staff plays an important role in the hospital: they implement and maintain various portions of the EHR systems. They have the ability to modify different technical features (such as those described above) that are meant to protect patient data. They are also responsible for customizing functionality and features to support different areas of the hospital. For instance, the set of features that are needed in the ED are different than in an in-patient unit or a surgical operating suite [12]. Therefore, the IT staff must work with users to customize the EHR for the particular unit and provide the appropriate privacy features that integrate with the users' collaborative work practices in that setting.

Despite their important role in supporting users and implementing effective privacy features in hospitals, IT staff members are often not considered in EHR studies because they are not the primary *users* of the system. There have been a number of studies focusing on understanding work practices from the clinical users' perspective [11,13–15] and more recently from the non-clinical users' [11,12,16–18] perspective. However, few studies have examined how well hospital IT staff understand the work practices of EHR users and how these work practices may impact patient privacy. Yet, understanding IT staff's perspectives is important for a number of reasons. Any misunderstandings between the IT staff's perception of user work practices and how they protect patient privacy and the users' actual work practices and how they affect patient privacy can result in a number of problems in the configuration, implementation, or customization of the EHR systems [19]. This gap can lead to collaboration challenges, interrupted workflow, and privacy breaches [11]. Without examining the IT staff's perspective, we cannot be sure that they understand their users' practices in a way that allows them to customize EHRs to best fit user needs while maintaining patient privacy.

In this study, we examine the role of privacy and EHR use in collaborative clinical work and how it is understood by hospital IT staff. Privacy is often defined as an individual state of limited access to personal information [20]. However, the focus of this research is not on the concept of privacy *per se.* Instead, we focus on privacy management problems resulting from medical work practices in terms of collection, sharing, distribution, and use of patient information. Concerns for confidentiality, integrity, and security usually occur at the stage in which patient data are collected and stored in database [21]. Even if the IT staff members implement appropriate mechanisms to ensure confidentiality, integrity, and security of patient data in the EMR systems, users could still make decisions about subsequent use and distribution of patient data that could result in privacy problems. Therefore, we argue that the task of protecting patient privacy includes not only ensuring the confidentiality, integrity and security of patient data, but also ensuring the appropriate use and distribution of patient information.

To better understand the IT staff's perspective as well as users' behaviors, we interviewed 20 IT staff members to examine their perceptions of EHR users' activities and of the tension between ensuring patient privacy and supporting their collaborative work. We also conducted observations of clinical and non-clinical EHR users in inpatient units of the hospital. The purpose of the observations was to understand the users' actual behaviors and activities when interacting with the EHR and how their behaviors and activities relate to patient privacy protection. We were interested in finding out if there were any gaps between IT staff members' perceptions of users' EHR use and how users actually used the EHR, especially regarding behaviors that protect or compromise patient privacy. To the best of our knowledge, this study is among the first to examine both perspectives of IT staff members and EHR users to understand the tradeoff between work efficiency and patient privacy protection. As such, it provides an alternative and useful counterpoint to user-level studies that have focused solely on EHR users.

2. Background

2.1. Collaborative work practices in healthcare

Researchers have stressed the importance of understanding collaborative work practices and the design of collaborative systems in clinical settings [2]. Most of these studies examine collaborative work practices and collaborative tools from the clinical user perspective. For instance, Ellingsen and Monteiro [13] studied how physicians' collaborative work practices were affected by the integration and lack of integration of HIT in various clinical settings and made design recommendations for collaborative information systems in hospitals. By conducting interviews and focus groups with physicians, and nurses, (and other users), Bossen [19] found a disconnect between work models represented in the EHR and actual clinician practices. Other researchers have studied how HIT impacts clinical users' informal work practices, such as during shift change among nurses [15,22]. For example, Tang and Carpendale [15] found that HIT weakened social interaction and interpersonal communication among clinical workers and made their work even more distributed. A growing number of studies also highlight the critical role of non-clinical staff in hospitals and the importance of considering non-clinical staff during HIT design and implementation [11,17,18]. Bossen et al. [17] examined how medical secretaries' work changed during EHR implementation and found that transcribing became more cumbersome, organizing records in a timely manner became frustrating, and their work practices became more interdependent.

IT staff members have not been the focus of many studies examining the implementation and use of EHRs. Few studies have looked at IT staff's perceptions of user practices in healthcare. Jaana et al. [23] conducted a survey of IT executives to better understand management issues in Canadian hospitals. They found certain key issues overlapped across different types of hospitals, such as recognizing IT as a key stakeholder in major hospital decisions, managing demands and expectations for IT services, and recruiting and developing IT staff with the appropriate skill set. Bossen [19] conducted interviews with IT staff members (in addition to physicians, nurses, secretaries, and social and health assistants) to examine how HIT fits actual work practices. However, they did not explicitly report their findings from interviewing the IT staff; rather their find-

Please cite this article in press as: E.V. Eikey, et al., Designing for privacy management in hospitals: Understanding the gap between user activities and IT staff's understandings, Int. J. Med. Inform. (2015), http://dx.doi.org/10.1016/j.ijmedinf.2015.09.006

Table 1
Summary of participants and data collection methods.

Participants	Roles/titles of participants (ID is provided for individuals who are quoted in the paper)		Data collection method	Amount
IT staff	Senior analyst	IT01/IT21,IT04,IT07,IT13	Semi-structured interviews	22 interviews (20 unique IT participants)
	Lead analyst	IT03/IT08,IT15,IT16,IT19		
	Systems analyst	IT12, IT14, IT20, IT22		
	Connected support	IT06		
	Informatics pharmacist	IT05		
	Project manager	IT11		
	System director	IT09		
	Computer network administrator	IT17		
		IT18		
	Director of infrastructure	IT10		
	Interface programmer	IT02		
	Educator			
EHR users	Attending physician	A02	Observations	155 h
	Senior resident	SR01		
	Resident	R03, R04		
	Medical intern	I04		
	Care coordinator	CC01		
	Nurses			
	Pharmacists			
	Social Workers			
	Therapists			

ings focused on the perceptions of clinical users. Chow et al. [24] examined how IT support impacted nurses' attitudes and found that having good IT support was linked to positive attitudes and satisfaction toward HIT. Other researchers have studied collaboration and knowledge sharing among IT staff members [25]. The dearth of studies examining hospital IT staff highlights a gap in our understanding of the various stakeholders in HIT design and implementation.

2.2. Privacy in healthcare

Many hospitals worldwide are required to comply with legal requirements that protect the confidentiality of patients' protected health information (PHI). In the United States, these legal requirements include the Health Insurance Portability and Accountability Act (HIPAA) [1] and Health Information Technology for Economic and Clinical Health (HITECH) Act [26]. HIPAA defines privacy rules that protect the confidentiality, integrity, and security of PHI and includes penalties for violations of the rules. HITECH expands HIPAA to state that any EHR system that stores PHI is held accountable to the security and privacy standards, as specified in the American Recovery and Reinvestment Act of 2009 [27]. These legal requirements have led to the creation of organization-wide privacy policies and the inclusion of technical privacy and security mechanisms in HIT systems.

Researchers have studied the design of privacy and security mechanisms of HIT within hospitals. These include role-based access controls, such as authentication mechanisms that use unique usernames and passwords to determine access to the system, and authorization controls that assign users to an appropriate role that determines the actions they can perform in the system (e.g., view, add, edit and delete) [4,28]. Additionally, privacy and security mechanisms of HIT systems also include the use of audit trails that track user activities [8] and encryption mechanisms that encode the patient information to prevent unauthorized viewing of the data [29]. In the *privacy by design* research, the importance of dealing with privacy issues early and embedding privacy features within systems is well known [30]. However, it is not always possible to understand how these privacy and security mechanisms will affect HIT users within highly collaborative and dynamic clinical environments, such as EDs and intensive care units (ICUs).

Current studies describe how implementing certain technical mechanisms may negatively affect clinical workflow and users' collaborative work practices [6,31]. Studying privacy practices of teams in the ED, Murphy et al. [11] found that various privacy safeguards impeded ED staff's workflow. Chen and Xu [32] argue that privacy features need to be properly aligned with users' activities and must be constantly re-evaluated due to the dynamic nature of healthcare. Since the IT staff members configure and implement HIT systems for the hospital, they play a critical role in evaluating these HIT security mechanisms and understanding how they align with users' collaborative work practices and privacy practices. Although current research identifies how privacy and security mechanisms impact users' work, there is limited research on the IT staff's understanding of how the privacy and security mechanisms impact their users' work. The research reported here seeks to address this gap in the literature.

2.3. Workarounds in healthcare

When the system configurations and the organization's privacy policies and procedures do not accurately reflect users' actual work practices, hospital staff may utilize workarounds to circumvent interruptions to their workflow [6,33,34]. Ash et al. [33] describes workarounds as clever alternative methods developed by users to accomplish what the system does not easily allow them to do. Morath and Turnbull [35] define workarounds as "work patterns an individual or a group of individuals create to accomplish a crucial work goal within a system of dysfunctional work processes that prohibits the accomplishment of that goal or makes it difficult" (p. 52). Hakimzada et al. [36] describes workarounds as "strategies or work patterns that bypass procedural codes in an effort to improve efficiency or productivity, but often with increased risk of error" (p. 170). Although some workarounds can be seen in a positive light [34], many of these workarounds are viewed negatively because they can result in inefficient, poor, or unsafe patient care [37–39], cause security breaches [37], and break both organizational policies and federal regulations [11,37]. Researchers have studied how the organization's policies and procedures can hinder hospital staff's work practices thereby resulting in workarounds [11,33,40]. For example, privacy policies in healthcare are often too vague to translate into day-to-day work practices [11]. Since these policies often do not account for the specific work practices of different groups

Please cite this article in press as: E.V. Eikey, et al., Designing for privacy management in hospitals: Understanding the gap between user activities and IT staff's understandings, Int. J. Med. Inform. (2015), http://dx.doi.org/10.1016/j.ijmedinf.2015.09.006

within the hospital, the policies may not be implemented consistently across these groups [11].

A number of studies have looked at how the mismatch between system design and clinical work in practice results in workarounds [6,11,37,41–44]. For instance, Yang et al. [42] used a case study approach to study the use of workarounds and their outcomes in a hospital. They found that physicians and nurses utilized a number of different workarounds to make their work more efficient. For example, physicians shared login accounts because of the slow login process, and nurses shared passwords to co-sign medications for other nurses because they felt the process was too cumbersome. Although technical mechanisms for logging on are meant to balance accessibility and privacy, Heckle and Lutters [6] found these mechanisms actually hindered user workflow in collaborative areas and resulted in the use of workarounds, which created security vulnerabilities and privacy concerns. Murphy et al. [11] found that when privacy safeguards interfere with the ED staff's collaborative work practices, they resort to workarounds, such as disabling timeouts and sharing passwords. While IT staff members cannot change the design of the system, they can adjust certain technical mechanisms to reduce unsafe workarounds.

2.4. Summary

As the background highlights, researchers in Medical Informatics, Human-Computer Interaction (HCI), and Computer-Supported Cooperative Work (CSCW) have examined a number of issues related to collaborative work practices, privacy, and workarounds in hospitals. However, most of these studies have focused only on the users of EHR systems. Therefore, we sought to understand the IT staff's perceptions of how users protect patient privacy while delivering healthcare and compare them to users' actual behaviors in order to understand what gaps may exist between the users and IT staff.

3. Materials and methods

3.1. Setting and participants

We conducted this study in a large academic hospital in northeastern United States, which has 551 beds, admits more than 25,000 patients per year, and has more than 47,000 emergency room visits per year. We employed two data collection approaches in the field study: interviews and observations. Specifically, we interviewed 20 IT staff members to understand their perceptions of EHR users' activities and the tension between ensuring patient privacy and supporting their collaborative work, and we also conducted observations of EHR users (both clinical and non-clinical) in the in-patient units of the same hospital (Table 1).

3.1.1. IT Staff participants

We interviewed the IT staff who support the implementation, customization, and management of the EHR system. We recruited participants through the hospital's Chief Medical Informatics Officer (CMIO), who sent out an email to all IT staff members asking for participation. We set up interview times via email with those who agreed to participate. Once we were on site, we also used snowball sampling by asking participants to let any IT staff member they thought could provide useful insights know we were available to speak with them. We interviewed 20 of 110 IT staff members from different areas of the IT department.

Since we were primarily interested in IT staff members who directly interact with users (i.e., through face-to-face meetings, video calls, phone calls, email conversations), 18 of the 20 participants were staff members who reported directly interacting with both clinical and non-clinical users. Many of our participants were part of the "Operational Group" (i.e., system analysts). Their job is to customize the technology for particular units and provide support around system releases and optimization. We also interviewed some IT staff members in management positions. Only 2 participants said they do not typically interact with users. These 2 participants stated they only get a sense of users' activities and needs post-implementation through indirect mechanisms, such as surveys.

3.1.2. User participants

We shadowed 5 Internal Medicine clinical teams in the in-patient units of the hospital. These teams included 5 attending physicians, 19 medical residents, and 5 medical interns. We also observed interactions between the clinical teams and other members of the patient-care team, including 60 nurses, 3 care coordinators, 2 social workers, and 2 pharmacists. The observations consisted of following the clinical teams' typical daily workflow, including activities, such as hand-off discussions between night flow shift and day shift, patient pre-rounds by the residents and interns, patient rounds with the clinical team, EHR documentation in the resident workroom, follow-up visits with patients in the afternoon (if necessary), and hand-off discussions with the night shift.

3.2. Data collection and analysis

3.2.1. Interviews with IT staff

Between April 2013 and January 2014, we conducted 22 semi-structured interviews (20 unique participants-labeled IT01–IT20; Table 1). We believed that semi-structured interviews were the best way to elicit the IT staff's thoughts about their users' work practices. Each interview lasted between 15 and 35 min. We audio recorded the interviews and also took interview notes and then transcribed the interviews for analysis. We stopped after 22 interviews because during our iterative process of data collection and analysis, we saw repetitive themes in the participant responses, and the interviews were converging into the same points (i.e., data saturation [45]).

In order to examine IT staff members' perceptions of users' activities and how their activities impacted patient privacy, we first had them discuss the concepts of privacy and collaboration and then had them consider the relationship between the two concepts. We asked questions about the participants' roles and responsibilities to understand their expertise and experience. We also asked participants about their interactions with HIT users. Then we asked them about tradeoffs of privacy mechanisms, user concerns or frustrations about the system, how they believe users deal with the tension between ensuring privacy while performing collaborative work practices, and workarounds.

We analyzed the interviews using general thematic coding [46]. During this process, we systematically reviewed the interview data to identify individual codes, which we then grouped into common themes found across the interviews (as shown in Fig. 1).

3.2.2. Observations of users

We also conducted 155 hours of observations of in-patient Internal Medicine clinical teams (i.e., attending physicians, medical residents, medical interns) and their interactions with other specialty physicians, nurses, care coordinators, social workers, therapists, and pharmacists between May and August 2014. The observations consisted of shadowing the clinical teams while they conducted their daily rounds. The observations lasted between 5-7 hours per session. We took field notes about the teams' patient-care activities, collaboration, communication of information, and documentation of information (informal notes and formal EHR entry). We also performed member-checking by asking the

Please cite this article in press as: E.V. Eikey, et al., Designing for privacy management in hospitals: Understanding the gap between user activities and IT staff's understandings, Int. J. Med. Inform. (2015), http://dx.doi.org/10.1016/j.ijmedinf.2015.09.006

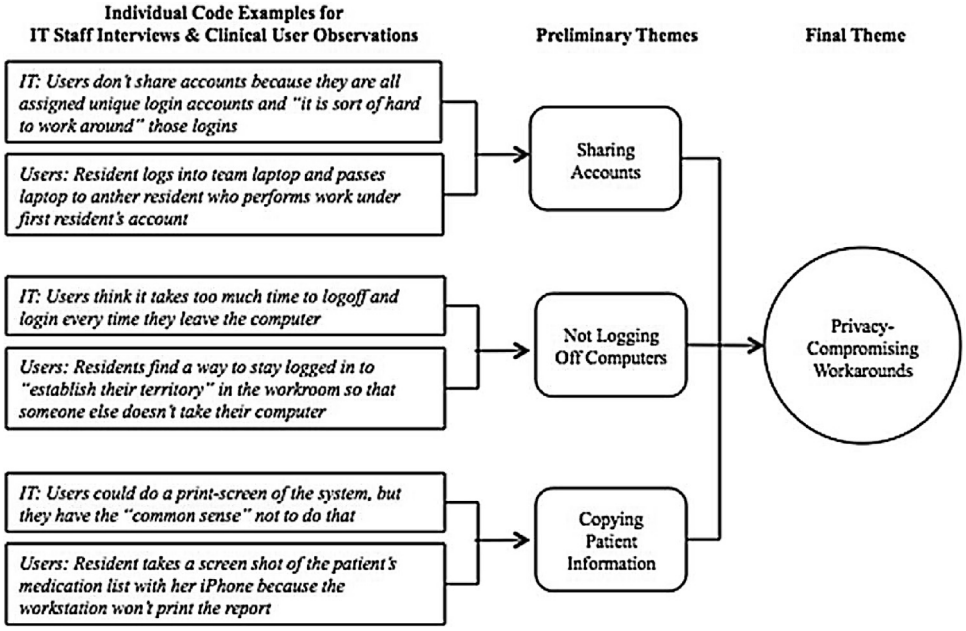

Fig. 1. Example of interview and observation coding process.

participants clarifying questions throughout the observations to affirm assumptions and provide additional information about their activities. The handwritten notes were then transcribed into an electronic format for analysis.

For this study, we analyzed the observational data by coding the data for workarounds, as well as user behaviors and activities that corresponded to the themes identified in the interview data. We then compared the perspectives of the IT staff and the corresponding user behaviors in order to generate the themes that are described in the findings section (as shown in Fig. 1).

4. Findings

As discussed above, various types of privacy mechanisms have been developed within EHR systems for vendors to achieve legal compliance. However, establishing privacy mechanisms that align with the "actual day-to-day procedures" remains one of the major challenges for healthcare organizations [47]. Prior studies provide evidence that users may see a need to improvise or work around privacy mechanisms in EHR systems. In this section, we discuss three forms of privacy-compromising workarounds identified through our field study that demonstrate the mismatch between what the IT staff thinks users do and what users actually do.

4.1. Information accessibility: sharing accounts

Clinical users, such as doctors and nurses, increasingly rely on the availability of patient information to provide treatment and make other clinical decisions. Information accessibility is very important in this context and it is often needed on a continuous basis. Consequently, researchers have pointed out that users sometimes share their accounts by either sharing passwords or their computer screens with one another in order to continuously access needed information even if it violates privacy protection policies [11].

While workarounds in healthcare settings are well documented [11,37,41,42], our IT staff participants had varying degrees of awareness about them being used in their hospital. A few IT staff members did not believe that users shared accounts as a workaround to logging into the system individually:

> *"No, uh, not that I am aware of...So you know, we were cautious in developing the security level and what each those levels could do, but also make sure we w*on't pro*hibit them from doing their job."* [IT05 interview]

> *"I don't think [users perform workarounds to access the system]. When they sign in, they have their unique logons that's not a generic login, so it's sort of hard to work around that. And the log off part of it, there is not really any way. . . I think we've pretty much covered making it secure."* [IT06 interview]

One IT staff member explained that users often perform workarounds for convenience and speed. However, this participant did not feel as though the system limitation impeded user workflow and collaboration enough to justify those workarounds:

> *"The only way [sharing accounts] would happen is if someone logs into a workstation and turns it and says, "Here you go." Which happens way more frequently than we're probably allowed to here [laughs], scary frequently. . .But in a live production system, my opinion is [sharing accounts] shouldn't happen. I mean, it takes, I would guess, less than 10 seconds to log in or even – [the HIT system] has a function called "change user," so you click a button and it shuts that chart, brings up a window, you type your stuff into it, and it switches to the next user. So, to me, there's no. . .I can't imagine that 7 seconds is that big of a difference. I don't know, maybe I'm wrong." [IT01 interview]*

This quote highlights a particular challenge about the mismatch between what the IT staff thinks users do and what users actually do. While the IT staff tries to understand the viewpoint of the users, many IT staff members believe the extra time required to log off and on is reasonable, especially given the importance of protecting the privacy of patient information. However, from the users' perspective, any added time or effort hinders their work and collaboration and they do not have an issue with sharing accounts at times. For instance, during the field study observations, we frequently observed the clinical teams sharing accounts while passing around a laptop during morning rounds. This was observed on a daily basis, and an example of one instance is provided:

> *During the morning rounds, a resident (R03) logs into the team laptop with his own credentials and pulls up the patient's record.*

Please cite this article in press as: E.V. Eikey, et al., Designing for privacy management in hospitals: Understanding the gap between user activities and IT staff's understandings, Int. J. Med. Inform. (2015), http://dx.doi.org/10.1016/j.ijmedinf.2015.09.006

He reviews the patient record on the laptop while walking down the hall. Once outside the patient's room, R03 hands the computer to another resident (R04) and R03 presents the patient's status to the clinical team based on information on his printed paper report. The attending physician (A02) recommends that they increase the patient's Tylenol dosage. R03 asks R04 if he can do that on the laptop. R04 says yes and puts in the request into the system under R03's account. [observational field notes]

In this case, it seems as though the IT staff are aware of users sharing accounts, but they believe that the time it takes to change user accounts is not an inconvenience. However, the IT staff did not appear aware of how users pass around laptops when entering patient orders, medications, or patient record changes during rounds. Yet, this appeared to be a normal activity for the users.

4.2. Operational resource limit: not logging off computers

Another common user activity is not logging out of their account when they are done using a computer or when they have to walk away from the computer. The IT staff are actually aware of this specific user behavior, which may potentially compromise the privacy of patient information. However, IT staff members state that the primary reason users do not log off is because of convenience and how long it takes to log back in:

"*The only thing I think is that they sometimes do*n't *log off. . .Nurses are working on the computers a lot so are tempted to stay logged on, and walk away, and. . .the breach is probably that somebody else will come up, do something with the patient, and it's not their login [account]. Cause you know, we'll have calls that'll say "I didn't do that with the patient." "Did you log off? Did you leave your computer open and one of your colleagues [used it]?". . .I don't think anybody's trying to do anything harmful. I think they're just thinking, "I want to try to stay logged on as long as I can because it's not a lot of fun [to log back in]."* [IT03 interview]

"Just the logging in and logging out, the time that it takes to do that, you know, when physicians think their time is. . .when they feel the pressure of getting into the system, doing their job, and getting out, you know, any of that extra time of logging in and logging out just. . .that to them, that to many people is an unreasonable expectation, but I think people are getting smarter about that too." [IT04 interview]

"On the mobile COWS [computers on wheels, typically located in hospital hallways], nurses will sign in, then they will do their work and walk away, and because you are in a public area, a patient's family is walking down the hall. For the privacy, we have to set a default time of when it will automatically log out. So somebody walking by doesn't see. And it is fine balance between being overly cautious and keeping the information private, and irritating the staff because [laugh], they say, 'I just walked away for a second and I have to log in again!' So, there are those types of settings on the system as well." [IT05 interview]

Although the IT staff are aware of this user behavior, they are not aware of *another* primary reason why users purposely do not log out of their accounts. During our observations, we repeatedly saw and heard that not logging out of a computer in the resident workroom was a common way for residents to "establish their territory" on the limited number of workstations available. This was described by a care coordinator who rounds with the clinical teams and observed during a workroom discussion:

"Yes, there's not enough computers in the resident workroom, so you'll notice that they try to get in real early to lock down a computer. It's funny, they'll leave themselves logged in and not log off to establish their territory, block their spot. So if someone else tries to use it, it will just show their account, sometimes even with things, reports or something that they're working on. So the other residents either respect it, or logs them off, which does not go over well! It's all about establishing their territory." [Care Coordinator (CC01), observational field notes]

The clinical team returns to the resident workroom. A senior resident (SR01) opens a computer and another user is still logged in. The previous user also left open a Word document with patient information on it. SR01 says, "Ah, this guy's trying to save his spot, block his workstation. Sorry buddy." SR01 starts reading the Word document and explains to the rest of the clinical team that the patient information in the document is for a patient on one of the other teams. The attending physician (A02) says the Word document was probably used to copy/paste patient information into a report in the EHR system. A02 then tells me "Write that down! Definitely a HIPAA issue. And it's a problem with using the copy/paste to do their reports too!" [observational field notes]

Without understanding the real reason behind why users employ privacy-compromising workarounds, the IT staff may waste their time and resources creating a technical solution that does not address the users' core issue with the HIT design. For instance, because the IT staff members think users stay logged on only for convenience, they may feel the "change user" feature, which allows a faster log out, adequately addresses the issue. However, as observed, it is not addressing the actual underlying problem of the residents "blocking their spots" due to a lack of workstations. Therefore, when considering the privacy practices of users, IT staff should seek to understand, as difficult as it may be sometimes, the different reasons for why users behave in certain ways. This can help address the gap between IT staff and users as well as provide insight into how to better address users' IT needs.

4.3. Workflow disruption: copying patient information

In the pursuit of privacy compliance, organizations implement features and procedures that may change the operational workflows. Users may not always positively react to implemented changes, especially when these changes disrupt their work routines. Failure to address the workflow disruptions could potentially lead users to employ privacy-compromising workarounds to bypass features that make accomplishing their work difficult. EHR systems are often designed with features that limit sharing and restrict unauthorized access to patient information. We asked IT staff if they were aware of users working around the restriction in order to share or copy patient information when needed for their work. Based on the responses, many IT staff members are aware of possible ways that users could do this:

"*I mean, we live in a world where everything's on the computer, so you could pretty much do a print-screen anywhere. So I mean if you wanted to, I want to say, there's ways around everything. If you wanted to you could do a print-screen on whatever and have that piece of paper in your hand and copy it and fax it and send it to the world. But. . .you know, common sense has to come in at some point."* [IT01 interview]

"Yeah, you can copy, you can screen-print, I mean there is a way around it" [IT05 interview]

Once again, many of the IT staff members are aware of user practices to work around restrictions in the HIT system, which prevent sharing or copying information. However, as with the previous section, the IT staff are not fully aware of the reasons why users employ privacy-compromising workarounds or all of the ways in which they do copy and share patient information from the HIT sys-

Please cite this article in press as: E.V. Eikey, et al., Designing for privacy management in hospitals: Understanding the gap between user activities and IT staff's understandings, Int. J. Med. Inform. (2015), http://dx.doi.org/10.1016/j.ijmedinf.2015.09.006

tem. For instance, we observed a medical intern using a personal phone to take a photograph of a patient's medication list because the printer would not allow the list to be printed or copied and the intern needed the list while speaking with the patient:

> *The medical intern (I04) enters the emergency department (ED) to transfer a new patient into in-patient. We go to the nurses' station and I04 logs into a "physician/consult" workstation computer to pull up the new patient's record. I04 reviews the patient's medications and attempts to print the medication list to discuss with the patient. The workstation will not allow I04 to print. I04 then takes out a personal iPhone and takes a photo of the medication list. I04 says to me, "Thank God for iPhones. I'll delete it later but I need it now, since we can't print."* [observational field notes]

Although the IT staff were aware that some users may take screenshots and print information that they should not be printing, they may not be aware of other ways users share information, such as taking photos of HIT screens with personal phones, which pose serious privacy risks. These issues are not always reported to IT staff and therefore, they are unable to get to the root of the real problem behind why users are copying or sharing patient information.

5. Discussion

Hospitals are highly collaborative environments that require staff members to work together to provide effective patient care. These complex environments require EHR systems that are designed to support the work practices of users while at the same time, protecting patient privacy.

This is a daunting challenge, and consequently, IT staff members must understand both *what* their users do and *why* they do it, especially regarding how users protect patient privacy during collaborative activities. The IT staff members need to constantly re-evaluate and understand the impact of technical mechanisms on the users' activities, especially in hospitals where people, technologies, and processes are constantly changing.

Fig. 2 shows the three forms of privacy-compromising workarounds that we have identified: sharing accounts, not logging off computers, and copying patient information to personal devices. These cases exemplify three factors that lead to workarounds: information accessibility, operational resource limit, and workflow disruption. Our findings reveal a gap in the IT staff's understanding of users' actual work activities, especially in regards to the privacy-compromising workarounds that are used and why they are used. IT staff members may have an incomplete understanding of users' work practices, and users may have an incomplete understanding of the challenges and limitations the IT staff face when trying to support users. The IT staff may not always understand the trade-offs that users face when trying to perform collaborative work while also ensuring patient privacy.

When the systems do not effectively support users' practices, users can become frustrated and use system workarounds to avoid workflow interruptions [48]. Although the hospital staff may view these workarounds as necessary, they can result in incorrect audit trails, inappropriate people accessing data or creating orders, and even privacy breaches. Some workarounds that compromise privacy can also have a negative impact on the patient-care process and lead to a cascading effect of more issues [34]. Although we found that users performed a number of different privacy-compromising workarounds, the IT staff were not always be aware of these workarounds either because they are unaware of the workaround altogether or because they have an incomplete or incorrect understanding about why users perform that workaround.

Since many of these workarounds can have negative consequences, the IT staff needs to identify the root cause of the workaround and find new solutions to mitigate the use of privacy-compromising workarounds. In order to ensure the IT staff are focusing on the actual issues so they can develop appropriate solutions, we need to improve both the IT staff's and the users' understanding of one another.

Below, we discuss three reasons why the gap between the IT staff members and users might exist, as well as how we may improve the IT staff's understanding of users' activities and how they protect patient privacy.

5.1. Communication between the IT staff and users

One issue is the limited interaction that the IT staff has with users after new system functions are implemented. While the hospital has an IT helpdesk with communication channels available for user feedback, according to the IT staff, there are not any policies regarding how feedback should take place, and they usually only receive feedback if there are access issues or needed critical changes.

After system features are implemented, the limited interaction and communication between the IT staff and users can result in a number of issues. First, some hospital staff may see some system limitations as an issue that they have to manage quickly on their own and therefore resort to workarounds that compromise privacy without reporting the limitation [50]. This may be one reason the IT staff has varying awareness of user workarounds and may not always understand the underlying problem. However, without users reporting these types of issues, the IT staff will not be aware of the problems and will be unable to make system adjustments that better fit user practices.

Second, while the IT staff receives little feedback from users post-implementation, the feedback they do hear is often complaints from users. Some explained that users express frustration over their role-based access, passwords, and timeouts. However, IT staff members we interviewed appeared to view these complaints as a result of user error or simple access problems instead of seeing the complaints as representing a larger issue of the system design not aligning with users' collaborative work activities.

So, how can the IT staff's understandings of users' collaborative work and privacy practices be improved? We believe part of the answer lies in improving the feedback mechanism from the user to the IT staff. In our study, IT staff members described the ways in which they receive user feedback during a project, and some IT staff members stated that there is a "culture" of not discussing the system with users post-implementation. So, the IT staff may not be aware of ineffective system design issues or the use of workarounds unless users report these issues to them and the IT staff consistently solicits feedback from the users about the systems' impacts to their work activities. Additionally, if these issues are serious, they then need to be escalated into formal changes to the system design.

Although the IT staff can only modify the parts of the HIT system that are configurable, other serious issues that cannot be changed in the off-the-shelf system need to be reported to the vendor to be considered as enhancements in future versions of the system. Therefore, user feedback is a critical part of configuring systems to adequately support the users' work, and hospitals should create effective communication channels for users to provide system feedback to the IT staff. Organizations that implement effective user evaluation or feedback channels can lead to the users having an improved perception of the systems that they use [51].

Even though some issues may not be able to be directly addressed by the IT staff, just improving the communication and understanding between users and IT staff can have a positive impact [24]. Building rapport and creating empathy can enhance per-

Please cite this article in press as: E.V. Eikey, et al., Designing for privacy management in hospitals: Understanding the gap between user activities and IT staff's understandings, Int. J. Med. Inform. (2015), http://dx.doi.org/10.1016/j.ijmedinf.2015.09.006

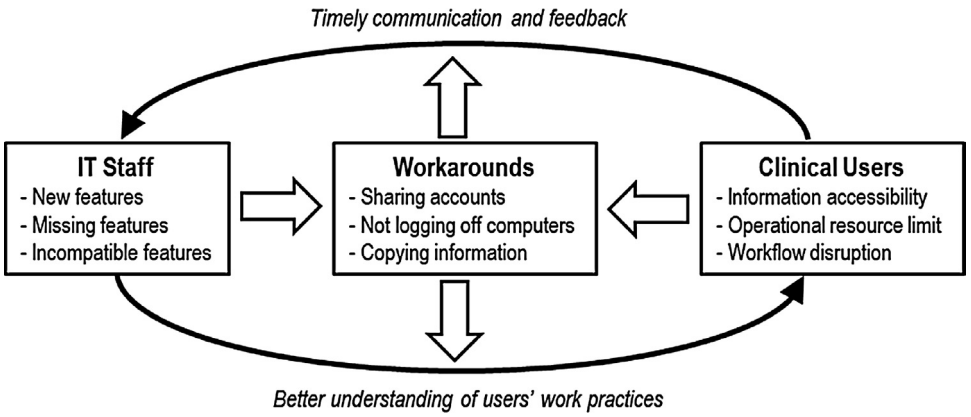

Fig. 2. Summary of research findings.

formance, promote innovation, and foster a better collaborative environment overall [52–54]. Perhaps this calls for a hospital IT position where someone shadows users periodically throughout the year in order to better understand their work and create rapport between users and IT staff. Additionally, this type of position could help identify needed changes to policies, procedures, and training.

5.2. IT staff's clinical training and education

Many IT staff members are not formally trained in the healthcare domain. While they may gain some knowledge from working within IT departments in hospitals, many aspects of hospital staff's work practices are beyond their experience or knowledge. In order to understand their users' workflow, IT staff members typically ask users questions about their needs and practices. However, users are not always able to articulate their actual work practices [55]. The IT staff modifies the system based on users' process descriptions without considering the difference between standardized processes and actual practices. Their lack of knowledge of user practices during the patient care process can make it difficult for them to translate user needs into effective system changes.

Although, many hospitals face this issue, changes are occurring in the composition of the IT staff that may begin to address this problem. One of the biggest changes is the increase in the number of IT staff members with clinical expertise. Additionally, nurses are increasingly becoming involved in the implementation and configuration of health information systems [56]. This is also happening with physicians as well as other allied groups such as pharmacists. The American Medical Informatics Association (AMIA) has also recognized the importance of addressing the gap between medicine and information technology by creating professional education and certifications for medical professionals, including physicians, nurses, and other clinical staff: "The need for informatics as an essential component of daily medical care and research cuts across all primary specialties" [57]. The incorporation of individuals with clinical expertise into the IT staff can help make the IT staff more aware of challenges that some users face, including how to better support users' collaborative work practices while maintaining privacy.

While hospitals are working towards incorporating more IT staff with clinical expertise into their departments, there are additional efforts that the hospital IT departments can employ in the meantime to lessen the gap between IT and users. For instance, in our study, care coordinators and pharmacists periodically rounded with the clinical team in order provide real-time expertise and support to the clinical team. This collaborative rounding generated a friendly rapport between the different roles and provided an opportunity for them to learn more about the challenges and issues that the clinical team experienced during their daily patient-care activities. Perhaps if IT staff members engaged in this type of collaborative rounding, they could learn about the actual user activities of the patient-care teams first-hand, including the use of privacy-compromising workarounds and the real reason for the workarounds. Additionally, the periodic presence of an IT staff member could also help develop an open, friendly rapport between IT and users so that feedback on system functionality and real-time support could occur on a continuous basis for the clinical teams.

5.3. User centered design

In order to better understand users' needs, there has been an increasing call for more emphasis on participatory design (PD) and user-centered design (UCD) of healthcare systems [51]. IT staff members in our study reported working closely with their users to understand their needs, reflective of an UCD approach.

Therefore, one important question is why are privacy-compromising workarounds still not effectively addressed in the design of EHR systems? Part of the answer is that privacy is often not at the forefront of user needs, especially because the primary focus for users is HIT features that help them perform their patient-care tasks. Consequently, privacy mechanisms play a secondary role to front-end capabilities of the system, such as the ability to access, document, and communicate information in an easy, user-friendly way. Therefore, users may not consider patient privacy as a primary function of any EHR system. Hence, even with PD and UCD approaches, users may be unable to offer input about privacy design mechanisms since many of these features are not visible to them.

Furthermore, given the complex processes involved in patient care, understanding what users actually need is a difficult task, as one IT staff member described. Zhou et al. [48] mentions that this gap between IT systems and users "reflects fundamental conflicts between medical practice and the design philosophy of healthcare systems." In our study, the IT staff stated their role is to add system features *specifically* asked for by the users. However, users may not always be able to articulate how to balance privacy needs with their work practice needs.

One approach to addressing this problem is to make privacy issues *explicit* during the UCD process. That is, instead of viewing privacy in purely technical terms (i.e., leaving it to the IT staff to implement), it should be viewed as a socio-technical problem that requires users and IT staff to work together to ensure that the privacy mechanisms adequately protect patient information but at the same time do not negatively affect users' work practices.

Please cite this article in press as: E.V. Eikey, et al., Designing for privacy management in hospitals: Understanding the gap between user activities and IT staff's understandings, Int. J. Med. Inform. (2015), http://dx.doi.org/10.1016/j.ijmedinf.2015.09.006

6. Conclusion

Hospitals are spending millions of dollars to implement EHRs in order to meet regulatory requirements [58]. These systems must not only support the collaborative work practices of their users but also effectively enforce patient information privacy rules. Consequently, a hospital's IT staff faces a daunting task in ensuring users' work activities are supported by the system while providing effective privacy mechanisms. In order to achieve both goals, the IT staff must have a clear understanding of their users' activities and how user work practices may impact patient privacy. However, as this study highlights, there is a gap between the IT staff's understanding of users' work activities and their actual work activities, especially regarding patient privacy. Specifically, the IT staff may not always understand why privacy-compromising workarounds exist and therefore may struggle to find appropriate solutions. We need to address this gap by improving both the IT staff's understanding of users' work activities and the users' understanding of the design rationale for privacy protection mechanisms.

By addressing this gap, we can then develop better approaches to implementing and configuring HIT that not only effectively support users' work activities but also ensure the patient information is protected. For instance, there is increasing interest in *privacy by redesign* [30], an approach which recognizes that privacy mechanisms should continually be reviewed and updated [32]. This approach might be useful for improving the effectiveness of privacy mechanisms in EHRs.

Furthermore, design should not only encompass the technical aspects of the system but also organizational policies and procedures that these systems support [49]. Some privacy-compromising workarounds may not necessarily be addressed through redesign of the system alone but rather through policy and procedure redesign. For example, the IT staff developed a quick "change user account" mechanism to the system that they believed addressed the problem of sharing accounts, which they thought was due to the login/logoff taking too long; however, as our findings show, despite the addition of this feature, users still did not log out when they physically passed around laptops. Because the IT staff has an incomplete understanding of why and how users share accounts, they spent time and resources developing a feature that did not fully address the problem. Even if IT staff removed the typing required as part of the login/logoff process by adding a card swipe or biometric authentication, users may still share accounts because they feel this is an acceptable practice. Therefore, with a better understanding of why and how users employ these privacy-compromising workarounds, the IT staff can decide if the issue is best addressed through system redesign or through training or policy redesign. If they determine adjusting technical mechanisms is not enough, then they can pass the information about the privacy-compromising workaround to others who can help address these issues from a training and policy standpoint.

While this research constitutes a step toward a better understanding of hospital IT staff's understanding of user activities and how users' work practices may affect patient privacy, it raises questions that need to be addressed in future research. As we shift from individual to collaborative work, we may need to rethink how EHR's privacy mechanisms are designed as well as how policies, procedures, and training around system use can impact privacy. We hope that the ideas and preliminary findings put forth in this paper will stimulate research on integrating the perspective of users with the perspective of IT staff, which remains a relatively unexplored area in our field.

Conflict of interest

None.

Summary points

What was already known on the topic:

- HIT is designed to enforce privacy policies.
- Workarounds are often used by hospital staff to circumvent HIT limitations.

What this study has added to our knowledge:

- IT staff play an important role in implementing HIT in hospitals but their knowledge of clinical user needs are sometimes limited.
- IT staff's perceptions of what users do and what users actually can be different.
- There is need for more effective communication between IT staff and clinical users.

Funding

We gratefully acknowledge the U.S. National Science Foundation for supporting this research (grant #IIS-1017247 and #DGE-1255832). Part of Heng Xu's work was done while working at the National Science Foundation. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Author contributions

Elizabeth Eikey conducted the interviews with the IT staff. She helped write the abstract, background, methods, findings, and discussion.

Alison Murphy conducted the observations with users. She helped write the background, methods, findings, and discussion.

Madhu Reddy helped conceptualize the study and paper. He helped write the discussion and conclusion. He helped with the abstract, background, methods, and conclusion as well as proofreading the paper.

Heng Xu helped conceptualize the study and paper. She helped with the background and the discussion points as well as Fig. 2.

We would like to thank the CMIO for his help and the IT staff and the clinical users for their willingness to participate in this study.

References

[1] U.S. Department of Health and Human Services. Health Information Privacy. (2013). Available from: http://www.hhs.gov/ocr/privacy/.
[2] G. Fitzpatrick, G. Ellingsen, A review of 25 years of CSCW research in healthcare: Contributions, challenges and future agendas. CSCW [Internet] (2012) p. 1–57. Available from: http://link.springer.com/10.1007/s10606-012-9168-0 [cited 2013 September 17].
[3] S. Bartsch, Exploring twisted paths: analyzing authorization processes in organizations, Proceeding-2011 5th International Conference on Network and System Security NSSS (2011) 216–223.
[4] L. Bauer, L.F. Cranor, R.W. Reeder, M.K. Reiter, K. Vaniea, Real life challenges in access-control management, in: CHI [Internet], New York, New York, USA: ACM Press, 2009, pp. 899–908, Available from: http://dl.acm.org/citation.cfm?doid=1518701.1518838.
[5] R. Heckle, W.G. Lutters, D. Gurzick, Network Authentication using Single Sign-On The Challenge of Aligning Mental Models (2008).
[6] R.R. Heckle, W.G. Lutters, Tensions of network security and collaborative work practice: understanding a single sign-on deployment in a regional hospital, Int. J. Med. Inform. [Internet] 80 (8) (2015) e49–e61, Available from: http://www.ncbi.nlm.nih.gov/pubmed/21398174 Elsevier Ireland Ltd., (2011) [cited 2014 December 22].
[7] Y. Chen, S. Nyemba, B. Malin, Detecting anomalous insiders in collaborative information systems, IEEE Trans. Dependable Secur Comput. 9 (3) (2012) 332–344.
[8] D. Fabbri, K. Lefevre, Explaining accesses to electronic medical records using diagnosis information, J. Am. Med. Inf. Assoc. [Internet] 20 (1) (2013) 52–60, Available from: http://www.pubmedcentral.nih.gov/articlerender.

fcgi?artid=3555324&tool=pmcentrez&rendertype=abstract January 1 [cited 2014 June 3].
[9] J. Bethencourt, B. Waters, Ciphertext-Policy Attribute-Based Encryption (2007).
[10] S. Narayan, M. Gagné, R. Safavi-Naini, Privacy preserving EHR system using attribute-based infrastructure, Proceeding 2010 ACM Work Cloud Computing Security Work—CCSW '10 [Internet] (2010) 47, Available from: http://portal.acm.org/citation.cfm?doid=1866835.1866845.
[11] A.R. Murphy, M.C. Reddy, H. Xu, Privacy practices in collaborative environments: a study of emergency department staff, CSCW 2014 (2014) 269–282.
[12] A.R. Murphy, M.C. Reddy, N. McNeese, Exploring the perceptions and use of electronic medical record systems by non-clinicians, in: Designing Interact. Syst. (DIS), Vancouver, BC, Canada, ACM Press, 2014, pp. 429–432, Available from: http://dl.acm.org/citation.cfm?id=2600884.
[13] G. Ellingsen, E. Monteiro, A patchwork planet integration and cooperation in hospitals, Comput. Support Coop. Work [Internet] 12 (February (1)) (2003) 71–95, Available from: http://link.springer.com/10.1023/A.1022469522932.
[14] J.E. Bardram, C. Bossen, A Web of Coordinative Artifacts: Collaborative Work at a Hospital Ward. Group '05, ACM, Sanibel Island, Florida, 2005, p. 168–176.
[15] C. Tang, S. Carpendale, Evaluating the deployment of a mobile technology in a hospital ward, in: CSCW [Internet], New York, New York, USA: ACM Press, 2008, pp. 205–214, Available from: http://portal.acm.org/citation.cfm?doid=1460563.1460596.
[16] N.L.H. Møller, S. Vikkelsø, The clinical work of secretaries: exploring the intersection of administrative and clinical work in the diagnosing process, in: J. Dugdale, C. Masclet, M.A. Grasso, J.-F. Boujut, P. Hassanaly (Eds.), From Research to Practice in the Design of Cooperative Systems: Results and Open Challenges, Springer, London, 2012, pp. 33–47.
[17] C. Bossen, L.G. Jensen, F. Witt, Medical secretaries' care of records: The cooperative work of a non-clinical Group. CSCW 2012. Seattle, Washington (2012), p. 921–30.
[18] J. Abraham, M. Reddy, Moving patients around: A field study of coordination between clinical and non-clinical staff in hospitals. CSCW (2008), p. 225–228.
[19] C. Bossen, Representations at work: A national standard for electronic health records CSCW New York (2006), P69–P78.
[20] H. Xu, H.H. Teo, B.C.Y. Tan, R. Agarwal, Effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: a study of location-based services, Inf. Syst. Res. 23 (4) (2012) 1342–1363.
[21] T. Dinev, H. Xu, J.H. Smith, P. Hart, Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts, Eur. J. Inf. Syst. [Internet] 22 (2013) 295–316, Available from: http://dx.doi.org/10.1057/ejis.2012.23 Nature Publishing Group.
[22] J.E. Bardram, C. Bossen, Mobility work: the spatial dimension of collaboration at a hospital, Comput. Support Coop. Work [Internet] 14 (2) (2005) 131–160, Available from: http://link.springer.com/10.1007/s10606-005-0989-y April [cited 2014 May 23].
[23] M. Jaana, H. Tamim, G. Paré, M. Teitelbaum, Key IT: management issues in Canadian hospitals, in: A Delphi study, the 44th Hawaii International Conference on System Sciences, 2011, pp. 1–11.
[24] S.K.Y. Chow, W.-Y. Chin, H.-Y. Lee, H.-C. Leung, F.-H. Tang, Nurses' perceptions and attitudes towards computerisation in a private hospital, J. Clin. Nurs. [Internet] 21 (11–12) (2012) 1685–1696, Available from: http://www.ncbi.nlm.nih.gov/pubmed/22081971 June [cited 2014 June 3].
[25] P.R. Spence, M. Reddy, Beyond expertise seeking: a field study of the informal knowledge practices of healthcare IT teams, Comput. Support Coop. Work [Internet] 21 (2-3) (2012) 283–315, Available from: http://link.springer.com/10.1007/s10606-011-9135-1 April 16 [cited 2014 June 3].
[26] U.S. Department of Health and Human Services. HITECH Act Enforcement Interim Final Rule (2013). Available from: http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html.
[27] U.S. Congress, American recovery and reinvestment act of. Public Law [Internet] (2009) p. 1–407. Available from http://www.gpo.gov/fdsys/pkg/BILLS-111hr1enr/pdf/BILLS-111hr1enr.pdf.
[28] S. Haas, S. Wohlgemuth, I. Echizen, N. Sonehara, G. Müller, Aspects of privacy for electronic health records, Int. J. Med. Inform. [Internet] 80 (2) (2010) e26–e31, Available from http://dx.doi.org/10.1016/j.ijmedinf.2010.10.001, Elsevier Ireland Ltd.
[29] J. Sun, X. Zhu, C. Zhang, Y. Fang, HCPP: Cryptography based secure EHR system for patient privacy and emergency healthcare. International Conference on Distributed Computing Systems (ICDCS) [Internet]. Ieee, 2011 [cited 2014 May 30] (2011) p. 373–382. Available from: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5961718.
[30] A. Cavoukian, M. Prosch, Privacy by ReDesign: building a better legacy, Inf. Privacy Commissioner Ontario (2011) 1–8, Available from https://www.privacybydesign.ca/index.php/paper/privacy-by-redesign-building-a-better-legacy/.
[31] D. Aronsky, I. Jones, K. Lanaghan, C.M. Slovis, Supporting patient care in the emergency department with a computerized whiteboard system, J. Am. Med. Inf. Assoc. 15 (2) (2007) 184–194.
[32] Y. Chen, H. Xu, Privacy management in dynamic groups: understanding information privacy in medical practices CSCW (2013) p.541–552.
[33] J.S. Ash, M. Berg, E. Coiera, Some unintended consequences of information technology in health care: the nature of patient care information system-related errors, J. Am. Med. Inf. Assoc. 11 (2) (2004) 104–112.
[34] M. Kobayashi, S.R. Fussell, Y. Xiao, F.J. Seagull, Work coordination, workflow, and workarounds in a medical context, in: CHI 2005 [Internet], New York, New York, USA: ACM Press, 2005, pp. 1561–1564, Available from: http://portal.acm.org/citation.cfm?doid=1056808.1056966.
[35] J.M. Morath, J.E. Turnbull, To Do No Harm: Ensuring Patient Safety in Health Care Organization, Jossey-Bass, Inc., 2005.
[36] A.F. Hakimzada, R.A. Green, O.R. Sayan, J. Zhang, V.L. Patel, The nature and occurrence of registration errors in the emergency department, Int. J. Med. Inform. [Internet] 77 (3) (2008) 169–175, Available from: http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=2259219&tool=pmcentrez&rendertype=abstract March [cited 2015 January 9].
[37] P.R. Zuzelo, C. Gettis, A.W. Hansell, L. Thomas, Describing the influence of technologies on registered nurses' work, Clin. Nurse Spec. [Internet] 22 (3) (2008) 132–140, Available from: http://www.ncbi.nlm.nih.gov/pubmed/18438162.
[38] M. Harrison, R. Koppel, S. Bar-Lev, Unintended consequences of information technologies in health care—an interactive sociotechnical analysis, J. Am. Med. Inf. Assoc. [Internet] 14 (5) (2007) 542–549, Available from: http://www.sciencedirect.com/science/article/pii/S106750270700165X [cited 2012 December 2].
[39] D.S. Debono, D. Greenfield, J.F. Travaglia, J.C. Long, D. Black, J. Johnson, et al., Nurses' workarounds in acute healthcare settings: a scoping review, BMC Health Serv. Res. [Internet] 13 (175) (2013) 1–16, Available from: http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=3663687&tool=pmcentrez&rendertype=abstract January [cited 2014 July 22].
[40] M.I. Harrison, K. Ross, B.-L. Shirly, Unintended consequences of information technologies in health care—an interactive sociotechnical analysis, J. Am. Med. Inf. Assoc. 14 (5) (2007) 542–549.
[41] S.A. Collins, M. Fred, L. Wilcox, D.K. Vawdrey, Workarounds used by nurses to overcome design constraints of electronic health records, Proceedings of the 11th International Congress on Nursing Informatics [Internet] (2012) 93–97, Available from: http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=3799185&tool=pmcentrez&rendertype=abstract.
[42] Z. Yang, B.-Y. Ng, A. Kankanhalli, J.W. Luen Yip, Workarounds in the use of IS in healthcare: a case study of an electronic medication administration system, Int. J. Hum. Comput. Stud. [Internet] 70 (1) (2015) 43–65, Available from: http://linkinghub.elsevier.com/retrieve/pii/S1071581911001042 Elsevier, 2012 January [cited 2014 July 22].
[43] J.J. Saleem, A.L. Russ, C.F. Justice, H. Hagg, P.R. Ebright, P.A. Woodbridge, et al., Exploring the persistence of paper with the electronic health record, Int. J. Med. Inf. [Internet] 78 (9) (2009) 618–628, Available from: http://www.ncbi.nlm.nih.gov/pubmed/19464231 September [cited 2015 January 9].
[44] R.J. Holden, Physicians' beliefs about using EMR and CPOE: in pursuit of a contextualized understanding of health IT use behavior, Int. J. Med. Inf. [Internet] 79 (2) (2010) 71–80, Available from: http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=2821328&tool=pmcentrez&rendertype=abstract February [cited 2015 January 9].
[45] M.N. Marshall, Sampling for qualitative research, Family Practice [Internet] 13 (6) (1996) 522–526, Available from: http://www.ncbi.nlm.nih.gov/pubmed/9023528.
[46] V. Braun, V. Clarke, Using thematic analysis in psychology, Qual. Res. Psychol. [Internet] 3 (January (2)) (2006) 77–101, Available from: http://www.tandfonline.com/doi/abs/10.1191/1478088706qp063oa.
[47] Y.B. Choi, K.E. Capitan, J.S. Krause, M.M. Streeper, Challenges associated with privacy in health care industry: implementation of HIPAA and the security rules, J. Med. Syst. [Internet] 30 (1) (2006) 57–64, Available from: http://link.springer.com/10.1007/s10916-006-7405-0 February [cited 2014 June 3].
[48] X. Zhou, M. Ackerman, K. Zheng, CPOE workarounds, boundary objects, and assemblages, in: CHI 2011 [Internet], New York, New York, USA: ACM Press, 2011, pp. 3353–3362, Available from: http://dl.acm.org/citation.cfm?doid=1978942.1979439.
[49] S.Y. Park, Y. Chen, Adaptation as design: Learning from an EMR deployment study. CHI′ 12. Austin, Texas, (2012) p. 2097–2106.
[50] J. Barnsteiner, Teaching the culture of safety, Online J. Issues Nurs. 16 (3) (2011) 1–14.
[51] G.B. Robert, Bringing User Experience to Healthcare Improvement: The Concepts, Methods and Practices of Experience-based Design, Radcliffe Publishing, 2007.
[52] W.A. Gentry, T. Weber, G. Sadri, Empathy in the Workplace: A Tool for Effective Leadership, Society of Industrial Organizational Psychology Conference. New York, New York, USA, 2007, pp. 1–16.
[53] D. McDonagh, J. Thomas, Rethinking design thinking: empathy supporting innovation, Australas Med. J. [Internet] 3 (8) (2010) 458–464, Available from: http://www.amj.net.au/index.php?journal=AMJ&page=article&op=view&path[]=391&path[]=631. August 30 [cited 2014 September 12].
[54] F. Miller, J. Wallis, Social interaction and the role of empathy in information and knowledge management: a literature review, J. Educ. Lib. Inf. Sci. 52 (2) (2011) 122–132.
[55] R. Cooper, S. Junginger, T. Lockwood, The Handbook of Design Management, A&C Black, 2013.
[56] H.N. Weckman, S.K. Janzen, The critical nature of early nursing involvement for introducing new technologies, Online J. Issues Nurs. 14 (2) (2009) 1–12.

Please cite this article in press as: E.V. Eikey, et al., Designing for privacy management in hospitals: Understanding the gap between user activities and IT staff's understandings, Int. J. Med. Inform. (2015), http://dx.doi.org/10.1016/j.ijmedinf.2015.09.006

[57] D.E. Detmer, B.S. Munger, C.U. Lehmann, Clinical informatics board certification: history, current status, and predicted impact on the clinical informatics workforce, Appl. Clin. Inf. [Internet] 1 (1) (2010) 11–18, Available from: http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=3631890&tool=pmcentrez&rendertype=abstract January [cited 2014 June 3].

[58] R. Brooks, C. Grotz, Implementation of electronic medical records: how healthcare providers are managing the challenges of going digital, J. Bus. Econ. Res. 8 (6) (2010) 73–84.

Please cite this article in press as: E.V. Eikey, et al., Designing for privacy management in hospitals: Understanding the gap between user activities and IT staff's understandings, Int. J. Med. Inform. (2015), http://dx.doi.org/10.1016/j.ijmedinf.2015.09.006