Privacy Practices in Collaborative Environments: A Study of Emergency Department Staff

Alison R. Murphy
College of Information Sciences and Technology,
The Pennsylvania State University
arm193@ist.psu.edu

Madhu C. Reddy
College of Information Sciences and Technology,
The Pennsylvania State University
mreddy@ist.psu.edu

Heng Xu
College of Information Sciences and Technology,
The Pennsylvania State University
hxu@ist.psu.edu

ABSTRACT
Privacy research has long focused on the individual. Yet most organizations are highly collaborative where teamwork is the norm. To examine privacy practices in collaborative settings, we conducted an ethnographic study of a highly collaborative and information-intensive setting – an emergency department (ED). We found that ED staff's work practices did not always align with the organization's privacy policies and procedures. We then discuss the use of workarounds when privacy policies interfere with work practices, the challenge of assigning accountability for enforcing privacy in collaborative environments, and implications for technical and policy design. We conclude with some thoughts on the future of privacy research in collaborative settings.

Author Keywords
Privacy; collaboration; collaborative privacy practices; privacy policy; privacy design; computer supported cooperative work.

ACM Classification Keywords
H.5.3 [Group and Organization Interfaces]: Computer-supported cooperative work; K.4.1 [Public Policy Issues]: Privacy.

INTRODUCTION
Privacy research has long focused on the individual. Most technological safeguards and policies have been oriented towards *individual privacy practices (IPP)* [22]. IPP studies have focused on users protecting the privacy of their own information while using technology [27, 28], managing the privacy of their own information when collaborating with others [6, 24, 26], and making decisions on individual privacy [11, 21]. Consequently, privacy mechanisms and underlying conceptions of privacy are still primarily focused on individual users' perceptions and behaviors [3]. Yet, in many organizational settings, collaboration and teams are an integral aspect of the work. Therefore, we need to investigate how privacy policies and technologies impact collaboration in settings where teamwork is the norm.

For a variety of reasons, hospitals are one domain of particular interest for examining privacy. First, collaboration and multidisciplinary teams are essential aspects of work in this environment. Yet, in these settings, it is often unclear who is responsible for the information. Is it the patient care team member who retrieved the information? Is it the team member who the information was shared with? Is it the team member who used the information? The actions (i.e., policies and technologies) taken to protect information privacy in an individual work setting will affect only that particular individual. However, in collaborative environments such as intensive care units or emergency departments, privacy policies and technologies may impact not only an individual but also the collaboration amongst individuals. Second, hospitals face a number of additional legal requirements because of the personal health information (PHI) that they deal with on a daily basis. In the United States, hospitals must comply with two important laws that focus on patient information privacy and security – Health Insurance Portability and Accountability Act (HIPAA) [45] and Health Information Technology for Economic and Clinical Health (HITECH) [46]. HIPAA details a set of privacy rules related to personally identifiable health information and the penalties for violations of those rules. HITECH expanded the HIPAA privacy rules by stipulating requirements for electronic medical record systems to be held accountable to the security and privacy standards specified in the American Recovery and Reinvestment Act of 2009 [47]. These laws have driven the development of hospitals' information privacy policies and technologies. Finally, hospitals are facing an increasing number of privacy breaches and the consequences of these breaches can be severe [44]. For patients, it may have adverse effects on medical insurance and employment. For hospitals, privacy breaches may lead

CSCW'14, February 15–19, 2014, Baltimore, Maryland, USA.

ACM 978-1-4503-2540-0/14/02...$15.00.
http://dx.doi.org/10.1145/2531602.2531643

to problems, such as reputation and trust damage, monetary penalties, and civil and criminal liabilities.

CSCW researchers have been examining the role of collaborative artifacts (e.g., electronic medical record systems, whiteboards), as well as the daily work practices of the hospital staff for a number of years [17]. However, while researchers have examined privacy in different settings [31], there has been little work on privacy related issues in hospitals. Therefore, we investigated privacy issues through an ethnographic field study of the patient-care team members in the highly collaborative and information-intensive environment of an emergency department (ED) in a large academic hospital in the U.S. In particular, we are interested in examining the question of how organizational privacy policies are managed in this busy, collaborative ED environment. To address this question, we have focused on *collaborative privacy practices* (CPP). We conceptualize CPP as a set of activities that a group or team undertake to maintain the privacy of the information that they use in their work. This conceptualization shifts our focus of privacy management from the individual to the group, where multiple stakeholders are responsible for co-managing the privacy of information.

In the next section, we describe the current privacy research in CSCW. We then present our research methods and an overview of the ED environment. In the following section, we present the results of our field study and highlight the privacy practices that facilitate privacy management in the ED. Next, we discuss the tension between work practices and organizational privacy policies, the challenges of assigning accountability for privacy in collaborative environments, and some design implications. Finally, we conclude with thoughts on the direction of future CPP research.

LITERATURE REVIEW

Within CSCW, the tensions of group-level privacy practices have been identified by Palen and Dourish through their discussions on the *reflexive interpretability of action* (how users understand how their actions appear to others) and *mediation* (how interaction with others is conducted via a computer mediated environment) [31]. However, collaborative privacy practices by medical employees are more complex because the healthcare sector is an information-intensive industry, and a large percentage of its activities are dependent on the storage, sharing, processing, transfer, and analysis of sensitive patient data. Very limited studies in CSCW have discussed the need for studying collaborative privacy practices [6, 11, 29], which includes studying the privacy behaviors of groups who co-manage and share information within medical settings [11, 29]. In medical environments, information is not typically about the information handlers themselves (e.g., doctors handling patient information). However, these handlers are responsible for managing and protecting the privacy of this information in a collaborative fashion. For this reason, the handling of patient information results in a shared (vs. individual) responsibility for protecting patient privacy, which is of critical importance to health practices and to society as a whole.

Protecting information privacy within a collaborative environment is challenging. This is because organizations must develop effective technical mechanisms that protect privacy, while trying not to restrict the collaborative use of co-managed data [4, 5, 20, 32]. Additionally, these organizations must also implement organizational privacy policies that may restrict access and use of confidential information, while trying not to impede the staff's ability to do their work [13]. This literature review summarizes current studies related to the implementation of these privacy mechanisms and privacy policies within collaborative environments.

Technical Privacy Mechanisms

Privacy mechanisms are used within organizations to protect the confidentiality of information. This includes the use of access control mechanisms [4, 5, 20], audit trails [10, 15], and encryption [8, 30]. Many of these studies highlight the challenges of designing privacy mechanisms for collaborative organizations. Bartsch [4] described how authorization mechanisms tended to be too rigid and did not account for the staff's information needs changing over time. Bauer et al. [5] also found issues with collaborative organizations' access control mechanisms because of a gap between those who designed the mechanisms and those who used them. In some cases, the systems did not have the technical capabilities to implement the required tasks. There were also concerns about developing effective access control and security mechanisms for highly sensitive information (e.g., patients' mental health records) while balancing the need for reliable information availability for important users (e.g., doctors) [37].

Additionally, a few studies have pointed out the importance of understanding organizational work practices before implementing new privacy mechanisms [4, 5, 20]. Heckle et al. [20] described how neglecting to understand the staff's work practices before implementing a new access control mechanism led to implementation delays, additional costs, and negative attitudes towards the technology itself.

Organizational Policies and Procedures

Privacy policies are written guidelines that are used to train staff on regulatory, legal, and organizational requirements for protecting the confidentiality of information. This is especially important in healthcare organizations where regulations, such as HIPAA, can restrict the use and sharing of important information. Choi et al. [12] discussed how the implementation of privacy policies that assure regulatory compliance inevitably decrease the "ease and efficiency" of

work practices. These privacy policies can even be in direct conflict with the work practices of the organization [38]. This can lead to serious issues, especially in healthcare organizations where restrictive policies can result in a negative impact to patient care [13]. A gap between policies and work practices can also result in the use of workarounds [1, 24]. These workarounds are temporary solutions that allow users to adapt technologies or processes in order to minimize interruptions [48]. However, the workarounds can deviate from the organizational policies, which could make the organization non-compliant with important regulations or laws.

There are also challenges in creating privacy policies for entire organizations. Turner & Dasgupta [43] described how the policies can become too generalized when including an entire organization within the same policy. These organization-wide policies can result in an inconsistent implementation of the policy within the separate groups.

These studies explore the impacts of both privacy mechanisms and organizational policies within collaborative environments. However, organizations cannot assure privacy based solely on the use of technical mechanisms and organizational policies [32]. The privacy practices of the staff must also protect privacy. There are studies that explore how employees' behaviors, or privacy practices, assure the confidentiality of information [35, 49]. Yet, these studies are limited and do not consider the impact that the privacy mechanisms and policies have on the work practices of the employees. Therefore, our study aims to better understand the collaborative privacy practices of the employees within a hospital's ED. This includes describing the impact that the organization's privacy mechanisms and policies may have on employees' privacy practices and work practices.

Summary

The need to balance the trade-off between privacy protection and work practices has been suggested by our literature review. However, within this body of literature, there lacks sufficient understanding of the underlying factors that determine the level of diligence of healthcare employees' handling patient information in their work practices. This is a significant exclusion because it is these medical employees who implement and comply with the technical and policy mechanisms to protect the privacy and confidentiality of patients' information. Therefore, we aim to gain an in-depth understanding about medical employees' privacy practices in terms of accessing, handling, and protecting patients' information in a collaborative environment.

In a recent interdisciplinary literature review, Smith et al. [39] have identified a lack of organizational privacy research in current literature, and the challenge is that organizational studies "are necessarily more complex and less conducive to 'quick' data collection techniques such as written and online surveys" (p. 1006). This gap in current privacy research has motivated us to conduct an ethnographic study to uncover the subtle organizational dynamics that drive privacy policies and practices.

METHODOLOGY

Research Site and Participants

We conducted this study in the ED of a large teaching hospital in northeastern United States. The ED has approximately 55,000 visits per year. The first author conducted 54 hours of observations and 4 hours of informal interviews with 7 clinical and non-clinical staff in the ED. We observed approximately 85 staff members, including: Physicians, residents, charge nurses, nurses, ED technicians, emergency medicine technicians (EMTs), pharmacists, transporters, care coordinators, social workers, registration assistants, chaplains, hospitality services, facilities, maintenance, and ED volunteers.

Phase	Description
(1) Familiarizing ourselves with the data	Transcribed interview notes and read transcriptions to ensure a general understanding of the data.
(2) Generating of initial codes	Labeled segments of data in a systematic way across all of the data.
(3) Searching for themes	Reviewed individual codes and identified preliminary themes.
(4) Reviewing themes	Reviewed preliminary themes to ensure they made sense across the entire data set.
(5) Defining and naming themes	Continuously refined each theme, identified a name for each theme, and defined the theme's boundaries.
(6) Producing the report	Presented themes with interesting examples that illustrate the individual themes.

Table 1: Braun & Clarke's six-phase thematic analysis approach

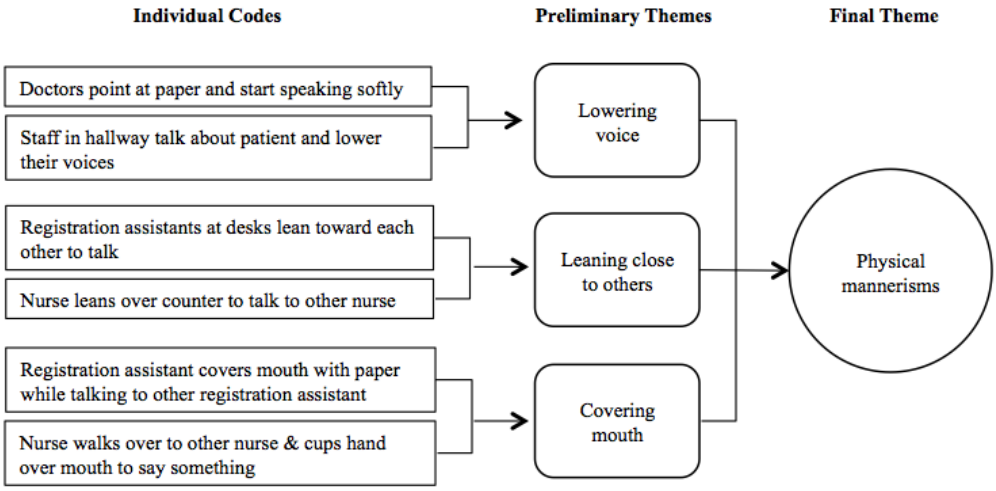

Figure 1: Example of theme generation using the thematic analysis approach

Data Collection

The 54 hours of observations were done in 2-5 hour increments over a 3-month period. Since the focus of the study was to understand the privacy practices of collaborative environments, we primarily focused our observations on two areas that had the largest amount of staff and information exchange: the registration area and the main nurses' station. We also observed the ED staff in hallways and at smaller nurses' stations. Detailed field notes were taken about the workflow, communication, collaboration, and technology use by both clinical and non-clinical staff. The field notes were then transcribed into an electronic document, resulting in 175 pages of data.

Data Analysis

The data was analyzed using Braun & Clarke's six-phase thematic analysis approach (Table 1) [9]. This general thematic analysis approach facilitates the process of becoming familiar with the data, systematically identifying codes and themes, and then defining and naming the common themes found across the entire data set. Through this analysis, we were able to identify types of privacy practices and mechanisms that helped facilitate privacy protection within the collaborative ED environment.

Figure 1 illustrates an example of how we generated individual codes, preliminary themes, and a final theme with this thematic analysis approach.

ED ENVIRONMENT

The ED is a fast-paced, collaborative environment where staff members have to work together to provide patient care. The staff includes clinical staff (e.g., physicians, residents, nurses, EMTs) and non-clinical staff (e.g., registration assistants, social workers, care coordinators, volunteers). The ED also sees a continuous influx of patients, visitors, and staff external to the ED (e.g., pharmacists, chaplains, specialized physicians).

Sources of Information

ED staff members received information from different sources. These sources included face-to-face communication, cell phones, pagers, desktop computers, laptop computers, computers-on-wheels (COWs), paper documents, white boards, and mounted electronic screens (e.g., tracking board).

The hospital policies state that the official patient medical records can be electronic, paper, or both; however, the ED used an EMR as its primary source of patient information. The hospital staff utilized computers throughout the ED to access the EMR. Desktop computers were found in patient rooms, nurses' stations, registration desks, and private offices. Some hospital staff (e.g., physicians, residents) carried laptops with them throughout the ED and used them to access the EMR at the nurses' stations and in private offices.

Some hospital staff frequently printed paper copies of patient records (called "face sheets") from the EMR. The staff carried these paper copies into patient rooms, took handwritten notes on them, and returned to their office computers to enter their notes into the EMR. When asked why they did this, they responded that it was more convenient and faster than having to log into the computer in the patients' rooms. They also stated that they preferred entering the patient information at their own computers to ensure that it was entered correctly into the system.

Organizational Privacy Policies

The ED staff had to attend mandatory training on organizational policies to make them aware of their responsibilities in protecting the confidentiality of patient information. The goal of these policies is to ensure that the hospital is in compliance with relevant federal and state laws and to protect the hospital from potential lawsuits. We reviewed 38 privacy policies that were part of the staff's

training. The topics of the organizational privacy policies included:

- Access, use, and disposal of patient information (paper and electronic)
- Disclosure of information electronically (e.g., email, facsimile, telephone, photograph, electronic medical record systems)
- Disclosure of information to external reviewers (e.g., business associates, auditors, court order)
- Protecting the security of information (e.g., virus protection, remote access, password management, vendor system review, security controls, modifications and testing of computerized systems, eStorage)
- Printing of patient information
- Individuals' rights for requesting amendments, restrictions on disclosure, and confidential communication of patient information
- HIPAA accounting of disclosures
- Reporting of privacy practice complaints

In this section, we summarize the organizational privacy policies that are relevant to the observed activities within our study (verbal communication, physical mannerisms, technical mechanisms) in order to provide contextual background for this paper.

Access, Use, and Disclosure of Patient Information

The policies state that staff should use discretion when discussing patients and their medical information, especially in areas that are public or not soundproof. Also, the access, use, and disclosure of protected health information (PHI) in verbal, paper, or electronic form must be restricted to the minimal amount necessary to perform job requirements.

Appropriate Use of Information

The policies state that staff should limit the viewing and use of confidential information to only authorized individuals by protecting confidential documentation, positioning computer screens in a way that limits the view, and logging out of active sessions after use.

Access to Electronic Medical Records

The policies state that the staff are assigned individually identifiable usernames and passwords after obtaining the required management approval. The staff must not share their usernames and passwords with others. Additionally, the staff must use their own unique accounts when accessing and performing actions within the hospital's EMR system. This is because the use of the individual's username and password becomes a digital signature for any action performed by that account (e.g., adding, editing, deleting data).

Access within the Hospital

The policies state that the staff are assigned photo identification badges after obtaining the required management approval, which are programmed to allow access to the necessary restricted areas. The staff must not share their badges with others and only use their own badges when entering restricted areas.

ED Workflow

The ED workflow begins when patients enter the ED as either a *walk-in* or a *trauma*. The walk-ins enter through the registration check-in area where registration assistants enter the patient information into the EMR system. The registration assistants collect the patient's name, date of birth, social security number, zip code, and complaint (i.e., symptoms). This EMR data entry process generates a patient ID and alerts the charge nurse and attending physician of the new patient so that they can assign a patient-care team. Physicians are assigned to one of three areas in the ED and nurses are assigned to specific rooms. The triage nurses evaluate the patient, if needed, and then take them to an ED room. Depending on the room and location of the room, specific ED physicians and nurses, along with the ancillary staff, form the patient-care team for that patient.

If there is a trauma, the patient arrives through the ambulance entrance where a registration assistant assigns a patient ID in the EMR and collects as much information as possible depending on the patient's state. The trauma patients are then immediately brought to one of the designated trauma rooms. The registration assistant also alerts the ED of the trauma by sending out a page to certain staff. The trauma page alerts the charge nurse and attending physician, who assign a patient-care team for the trauma. The trauma page also alerts the registration assistants in the check-out registration area, who post the trauma information on the EMR's "tracking board" and compile a "trauma pack" depending on the type of trauma (e.g., dead-on-arrival, brain attack). An assigned nurse or ED technician pick-ups the trauma pack from registration and proceeds to the trauma room where the patient-care team is briefed on the patient's status.

Once the patient is in his/her ED room, the assigned physician and nurse(s) perform their patient care activities (e.g., evaluation, tests, medication administration, treatment). Registration assistants also visit the patient rooms to gather additional registration information, including demographic, insurance, and contact information. The registration assistants collect this information on a paper "face sheet" and then enter the information into the EMR back at their desk. A care coordinator is assigned to help the patient with financial assistance options, patient training, and external facility coordination (e.g., rehabilitation, assisted living). If the patient has any issues with drug, alcohol, or physical abuse, or psychiatric concerns then a social worker is assigned. Additionally, if the patient requests spiritual support, a chaplain is assigned

as well. All members of the patient-care team log their activities in the EMR's "interdisciplinary narrative." This narrative is a real-time, chronological list of short updates about the patient's lab results, medication administration, and general assessments by the patient-care team. The physician and nurse also enter the patient's medical information into the EMR throughout their patient care activities. When patient-care team members need to discuss the patient, they frequently have the discussion at the main nurses' station that is centrally located in the ED.

If a patient receives visitors during their stay, the visitors arrive through the check-out registration area. The registration assistants provide the visitors with access to the ED. If the visitors are family members and the patient's registration information is not complete, then the registration assistants may ask the family members if they know the missing registration information (e.g., insurance, date of birth, address, phone number). The registration assistants then give the visitor the patient's room number and directions to the room. Visitors enter and exit through the access-controlled doors of the registration area.

When a patient is ready to be discharged, the patient-care team creates a discharge plan based on whether the patient will be admitted to the hospital, discharged to an external facility, or allowed to go home. Once the patient is discharged, the registration assistants check the patient out of the ED by logging his/her exit in the EMR and requesting any incomplete registration information.

FINDINGS

Sharing patient information is an integral part of patient care in the ED. However, because of the sensitive nature of patient information, there were various practices used to protect the privacy of this information. Through our analysis, we identified various privacy practices. We also identified several instances when organizational policies interfered with work practices. In these cases, the work practice was favored over the organizational privacy policy.

Types of Patient Information

The ED staff shared various kinds of patient information with one another.

- *Protected health information* (*PHI)* – Any specific medical information about a patient (e.g., the patient's symptoms, medications, test results, diagnosis);
- *Personally identifiable information* (*PII)* – Any information that could individually identify a patient (e.g., the patient's full name, date of birth, social security number, phone number, address);
- *Generalized information* – Any information that does not individually identify a patient or relate to his/her medical condition (e.g., the patient's food request, room number or location, physical description).

The staff members shared these three types of information in different ways. PHI was frequently discussed by all staff members because it was required by the patient-care team to determine a care plan for the patient. Yet, at the same time, staff members were typically more careful about openly discussing PHI with one another because of the confidential nature of the information.

PII was generally only discussed by the registration assistants because they were required to obtain demographic (e.g., ethnicity, age, gender, marital status) and identification information (e.g., social security number, phone number, address) from the patients. PII was openly discussed in the registration areas, but rarely shared anywhere else in the ED.

The generalized information was openly discussed by all ED staff. Since it was not personally identifiable information or sensitive medical information, there was little effort by the ED staff to protect the privacy of this information.

Privacy Practices

We observed various practices and mechanisms in the ED used to protect the privacy of patient information. These included physical mannerisms, secure spaces, physical proximity, ED access control, and information access control.

Physical Mannerisms

One of the primary methods of sharing information in the ED was verbal communication. The ED staff would frequently use certain physical mannerisms to prevent other individuals from overhearing their discussion. These practices included: lowering their voices, leaning closer to the person they were speaking to, and holding up their hand or a piece of paper to cover their mouth when speaking.

Two registration assistants are at their computers talking about three traumas that just arrived in the ED. The traumas were all children in the same family. One registration assistant describes to the other how the children's mother was outside the patient rooms crying and talking on her cell phone. She starts describing the medical state of the children. She then takes the piece of paper she's holding, puts it over her mouth, lowers her voice, leans into the other registration assistant, and continues to talk so that no one else in the area can hear them.

By putting the paper over her mouth, the registration assistant prevented visitors from hearing what she was saying. Her physical mannerism was also a signal to the other registration assistant that she was going to share some private information (i.e. PHI) about the case. This also made the second registration assistant more focused on the information that she was receiving.

Secure Spaces

ED staff also utilized what they considered secure spaces to share private information. For instance, although the registration desk and nurses' stations were open to the general hallways, there were a number of private offices

available for use. One office was located through the nurses' station and was called the "physicians' area." Many times physicians would leave patient rooms and return to the physicians' area to have conversations with other patient-care team members. Registration assistants also used a back office in order to have private conversations:

During a shift change at the registration desk, a new registration assistant comes in and starts talking to the others about what has been happening in the ED that morning. Another registration assistant in the back office asked the new registration assistant to come into the office to "discuss a few things." They go into the office and close the door.

By using the private office and closing the door, the registration assistants were able to have a private conversation that could not be heard by the visitors in the waiting room and by other registration assistants at the desk.

Additionally, there were open spaces within the ED where the staff thought it was appropriate to talk about patient information. One of these designated areas was the main nurses' station. The nurses' station is a centralized location where various members of the patient-care team can meet, document and obtain information from the computers and phones, and create the patient-care plans. Around the nurses' station, patient-care teams would frequently talk about generalized information and PHI, since they had to discuss medical information; however, they took care not to discuss PII, which would identify the patient. Team members openly discussed patient conditions, tests, or diagnoses with other ED staff around the nurses' station counter.

A physician and four residents exit a patient's room. They gather around the main nurses' station counter and the physician summarizes the patient's condition based on the examination. He also mentions the patient's current medications. The residents take notes in their notebooks. The physician then asks them what tests they think should be run on the patient. The residents offer their opinions and the physician discusses the recommended tests with the residents.

Other ED staff just walked by the group or continued their own work at the nurses' station without paying attention to the discussion about the patient.

One area that was not considered a secure space was the open hallway. If the ED staff were in the hallways, they would frequently use physical mannerisms to protect PHI or go to a secure space to talk about patients. However, there were times when ED staff openly talked to patients about PHI in the hallways.

A patient with a neck brace is walking in the hallway and passes two registration assistants. One registration assistant asks how his neck is doing. The patient mentions that it's a bad neck sprain from the car accident and that he has to wear the brace for two weeks.

In this case, the registration assistants are expressing emotional support, which could be considered part of their job. However, showing support by talking about PHI in an open hallway does not align with privacy policies on protecting the confidentiality of the patient's health information in open spaces. In this case, the registration assistants prioritized their work practices over the organization's privacy policies in order to express their concern about the patient's condition.

Physical Proximity

ED staff members also protected the privacy of information sources. In any area where computers were visible from the general hallways, staff members either stayed close to the computer where they were logged in, or they logged out before leaving the area to ensure that private information was not left open.

The main nurses' station also had a charge nurse's area with an outward facing computer that did not timeout. This lack of timeout did not follow the organizational privacy policy, which states that computers will automatically logout after a certain period of inactivity. However, this was not the case with the charge nurse's computer. Although this information was left open, the charge nurse and other nurses were always very close to the open computer to prevent unauthorized individuals from accessing the system and viewing PHI.

The charge nurse has been standing by her computer all morning. When she has to speak to other nurses, she calls them over to her computer. When a trauma arrives in the ED, the charge nurse is called away for a meeting. The charge nurse asks another nurse to stay at the computer while she is away. The other nurse then takes over standing at the charge nurse's computer.

It seems that physical proximity was used as an important method of protecting the privacy of patient information.

ED Access Control

One of the primary ways of maintaining privacy was through controlling access to the ED. All six entrances into the ED, except for the main entrance where patients checked-in, were access-controlled. There were also four access-controlled doors internally that connected the registration areas to patient room hallways. ED staff used their badges to open the doors themselves or the registration assistants opened the door for patients, visitors, or external hospital employees. In addition, the lead registration assistant watched a video monitor of the doors that provided visibility of any attempts to enter the ED. Registration assistants also had to use a code to enter their own office, which contained confidential paper records and fax machines.

However, on occasion, the registration assistants opened the access-controlled doors for other employees (e.g., nurse who forgot her ID, nurse pushing a wheelchair, nurse with her hands full).

A nurse pushes a patient in a wheelchair through the registration area. A registration assistant at her desk looks up, sees them, and pushes a button to open the door that the nurse is walking towards. The door swings open for the nurse and patient. The nurse thanks the registration assistant for opening the door for them. The nurse and patient proceed through the door.

According to organizational privacy policies, the nurse was supposed to badge herself in so that the hospital has an accurate record of entry into restricted areas. However, clearly, she had difficulty doing this while pushing a patient, so the registration assistant did it for her. The opening of doors for other ED staff does not follow the organizational privacy policy for controlling access to the ED. Instead, the registration assistants chose to assist their colleagues by opening the doors. This is another case where privacy policies did not align with work practices, and the work practices took priority over the policy.

Both registration assistants and staff around the nurses' station also controlled access to the ED by frequently approaching people they did not know. They would ask unknown individuals whom they were visiting and if they needed help with anything. This included asking the researcher conducting the observations why she was there, as well as other visitors or staff in the hallways and waiting areas. For example, the charge nurse approached an unknown individual who was behind the nurses' station:

The charge nurse walks up to a person who just entered the nurses' station. The charge nurse introduced herself and asked who the person was. The person identified themselves as an inpatient staff member of the hospital. The charge nurse then said, "Oh okay, I had just never met you before."

Talking to unknown individuals helped to control access to the ED and protect the privacy of patients by ensuring only appropriate people were in the ED.

Information Access Control

The access control mechanisms built into the ED computers also helped to protect the privacy of information. These computer mechanisms include unique logins, inactivity timeouts, and disabling user access after too many incorrect attempts to login.

A registration assistant sits down at the registration desk and mentions that she cannot log into the system. She says she believes she is locked out because she keeps forgetting her password and entered it incorrectly too many times. Another registration assistant tells her to "call the helpdesk right away" so that she can get it fixed and get back into the system.

There were also computer mechanisms that protected information at the nurses' station. The main nurses' station was situated in the middle of the ED in an arc shape with a high counter on the exterior of the station for staff members to use for writing or working. There were six "Physician/Consult" computers on the nurses' station counter facing outward towards the ED hallways for physicians, nurses, and other ED staff to use during their daily work. These monitors included authorization mechanisms, which required a general password to login to the desktop. A nurse said that these general passwords "*change regularly*." These systems then required a unique username and password to login to the EMR system. We also observed that these monitors automatically logged out after approximately 10 minutes of inactivity. All other laptops and monitors in the ED were located behind the nurses' station and within patient rooms and offices, which could not be easily observed from the hallways.

There were times when the daily work practices would not align with the organizational policies. On occasion, nurses at the nurses' station would openly share the general password to log into the "Physician/Consult" monitors. This was not a password to the EMR system itself, but for accessing the computer at the nurses' counter. Although the organizational privacy policies state that users should not share passwords, nurses had to often share the password in order to continue doing their work. The nurses viewed the risk in this situation as low because the password could only open the monitor and they also recognized the person they were giving the password to as an authorized ED employee.

In another situation, a registration assistant entered information about a trauma patient into the EMR on another registration assistant's computer.

A registration assistant returns from getting information about a trauma patient. He begins entering the information into the system and asks the other registration assistants at their desks certain questions about how to enter the trauma data. He then says that he is late for a meeting. Another registration assistant offers to finish the data entry and says, "Want me to just do it on yours?" The registration assistant then sits down at the other registration assistant's computer and finishes entering the information.

In this case, the registration assistant entered information under another registration assistant's account. This is a clear violation of the organizational privacy policy that states that all staff must use their own unique accounts when performing actions in the system (e.g., adding, editing, deleting information). This illustrates another time when the work practice was prioritized over the organizational policy. In this case, the registration assistant had to input the patient information in a timely manner because the patient was a trauma case and the other patient-care team members needed that information as soon as possible.

DISCUSSION

The privacy of patient information is a priority to hospitals. Not only are U.S. hospitals legally required to protect patients' privacy because of HIPAA and HITECH compliance [25, 45, 46], but properly managing privacy also builds trust and improves communication between providers and patients [27]. Therefore, hospitals often develop organizational privacy policies based on legal requirements to define how the employees should protect the privacy of patients' medical information [38].

However, the existence of a law does not automatically translate into an explicit organizational privacy policy. Consequently, these policies can range from being very specific to very general. For example, our study hospital had a very specific policy about technical access control mechanisms at the system level. This policy had clear instructions for the assignment of unique usernames and specific requirements for creating secure passwords to use when logging into systems. This policy also had specific guidelines on the use of security mechanisms, such as automatic logout after a specific time of inactivity and system audit trails that capture who created, modified, or deleted information with the date and time of the action. However, other behavioral aspects of privacy policies were more vague. An example of this is a hospital policy about the verbal communication of patient information. This policy generally instructed the staff to use their own discretion when discussing patients and their medical information, especially in public areas, and to only discuss the minimum amount of information required to do their work. These vaguely written policies made the medical staff more aware of privacy requirements, but did not provide explicit guidelines.

Often, these policies are written for the entire hospital and not just one particular unit. Therefore, the policies do not necessarily account for the different activities and work practices in the different units. So, a busy unit, such as the ED, has to deal with same policies as a less busy unit, such as floor ward. Consequently, the staff of the particular unit has to develop approaches to manage these privacy policies in the context of their own work setting.

Our findings suggest a lack of clarity in translating some of those abstract policies into day-to-day work practices. One potential consequence of the ambiguity in the organizational privacy policies is the staff's use of workarounds to deal with specific privacy policies that affected their work practices. In this section, we will discuss several underlying factors for explaining the workarounds observed in our study. We will also discuss the accountability for privacy within highly collaborative environments and design implications based on our findings.

Privacy Policy Workarounds

Studies have highlighted the demanding and busy nature of the ED [1, 36]. In this environment, the ED staff often resorted to workarounds to deal with breakdowns or other problems in the unit [1]. This was also the case in our study when the organizational privacy policies or security mechanisms interfered with the staff's work practices. In particular, the staff used privacy workarounds in order to have constant access to information and to improve work efficiency.

Constant Information Access

From an organizational perspective, allowing employees to stay logged into an unattended computer can create a wide variety of problems ranging from allowing individuals unauthorized access to the information to disrupting the audit trail of who entered the information. Therefore, most systems have automatic logout mechanisms to prevent these problems. Yet, this may also create unintended problems, such as increasing the time it takes to access the information. In the ED, all the computers except one had an automatic logout feature. This computer with no auto-logout was at the nurses' station and was frequently used by the nurses. This seemed to clearly violate the organizational policies on automatic timeout. However, the ED staff had created a workaround, as described in the findings, to ensure the privacy of the information. The staff used *physical proximity* as a privacy mechanism for ensuring that only authorized individuals had access to the information. The charge nurse or other nurses always stood close to the open computer. The charge nurse even specifically asked another nurse to stand close to the computer when she had to step away. Therefore, in this workaround, the technical safeguard (automatic timeout) was replaced with a human safeguard (physical proximity). This allowed the information to be protected while at the same time assuring staff access to the information that they needed without disrupting their work practice by having to constantly log back into the computer.

In a dynamic and demanding environment like the ED, a patient's condition could change from moment to moment and the medical staff has to be able to quickly respond to this change. If the information needed by the medical staff to make urgent clinical decisions was unavailable due to strict access control, patients may miss the best treatment opportunities. Therefore, one of the major challenges in the ED is to ensure that information is available to the staff at a moment's notice. Yet, the need for constant information availability in the ED does not align with the hospital's privacy policies about automatic computer logouts. As Salomon et al. [37] pointed out, achieving a balance between constant information access and privacy compliance becomes particularly challenging in a medical context. Failure to address clinicians' information needs could lead to them using workarounds to bypass privacy protection mechanisms (e.g., automatic timeout features).

Improve Workflow Efficiencies

Another issue in the ED is the number of interruptions that affected the workflow in the unit. In the pursuit of privacy

compliance, organizations enforce policies and technologies that may interrupt workflows or work practices. As a result, employees may not always comply with these organizational privacy policies and sometimes they try to minimize negative impacts of these policies on their work efficiencies through workarounds. For example, the hospital's privacy policy requires that ED staff badge themselves into any access-controlled areas so that the hospital can maintain an accurate record of who enters restricted areas in the hospital. However, there were times when registration assistants opened doors for other ED staff members who were supposed to use their own badges. The registration assistants performed this workaround if staff forgot their badges, were pushing a cleaning cart or wheelchair, or had their arms full. This workaround helped improve their work efficiency, but at the same time resulted in the inability to accurately track staff entry records.

Organizational privacy policies on data access/entry often conflict with the need for getting things done quickly in the ED. Similar to many organizations, the hospital's policy was that staff must enter information under their own username since that is the name associated with the entry in the audit trail. However, as described in the findings, we observed a situation where a registration assistant sat down at another registration assistant's computer to finish data entry for a patient. Getting the information into the system was a high priority because it was for a trauma patient and the trauma team needed access to any patient information as soon as possible. Yet, this was clearly in violation of the organizational policy on data access. However, the time saved by entering the information into the system under the other registration assistant's account instead of taking the time to save the information, log out the previous user, log back into the system, and find the patient record again outweighed the policy.

Similar to Smith [38], our study identified a "policy/practice gap," in which the staff's actual work practices are at variance with the official privacy policies. Negative effects of implementing privacy technologies and procedures on workflow and work efficiencies have been documented in the literature [12, 13]. Lovis et al. [26] identified one of the biggest challenges in privacy compliance in the medical context is to develop technologies and procedures that do not hinder the workflow and work practices of clinicians. In situations where privacy enhancing features and procedures disrupt their work efficiencies or workflows, staff try to minimize these negative impacts through workarounds to bypass privacy safeguards [1, 24]. Unattended workarounds can be potentially harmful to the overall organizational privacy compliance.

Accountability for Information Privacy in Collaborative Environments

Although there were situations where accountability for privacy violations was clear, there were a number of situations where it was not as obvious. For instance, in one case, the charge nurse asked another nurse to watch the no-logout computer while she left the area. In this case, the charge nurse clearly stated and assigned accountability to that nurse. However, in another situation, a registration assistant entered information under another registration assistant's account. In this case, it was not as clear about who was responsible for following the proper data entry policy. Was the first registration assistant responsible for logging out of the system before leaving the computer? Or was the second responsible for logging the previous user out of the system and logging back into the system with her own username and password? Or both?

The registration case illustrates how it is sometimes difficult to determine clear accountability in a collaborative environment where multiple people may be interacting with the same technologies. The first registration assistant may have assumed that the second would log out before continuing, while the second registration assistant may have assumed, based on previous practice, that she could use the account. Therefore, breakdowns in enforcing organizational policies can occur when there is ambiguity regarding who is accountable for privacy.

An additional issue to consider in collaborative settings is that the privacy practices may vary from person to person, which could create conflict or tension among the multiple information handlers. For example, certain areas of the ED were considered secure spaces to openly discuss private information. Physicians exited patient rooms and started openly discussing private patient information around the nurses' station. In this case, the physicians felt that they could freely discuss that private information because they were in a controlled-access ED around an area designated for other members of the patient-care team. However, it is possible that other ED staff members may not agree that physicians should be talking about private patient information in this area because visitors often walk by that area. They may believe that conversations about patients should occur in the private physicians' area located behind the nurses' station so that other patients and visitors do not hear the information being discussed.

In the ED, multiple staff members may access, use, and share a single patient's record. Therefore, staff members may have differing assumptions about whose responsibility it is to protect the privacy of that information. This is especially true when shifting privacy management from physical environments to computer-mediated environments [33]. There can also be overlapping accountability of specific privacy tasks, especially within fast-paced, highly collaborative environments such as EDs. All of these issues raise the question of who should be held accountable for managing the privacy of information.

Design Implications

In busy, information-intensive, and collaborative environments like the ED, it can be challenging to implement privacy policies that do not hinder the work

practices of the staff. In this section, we discuss some technical mechanisms and policy mechanisms that could help address some of these challenges.

Technical Design

The ED staff used workarounds in order to improve their access to information. This included disabling the automatic timeout mechanisms to avoid repeatedly logging into the system, becoming locked out of the system because of forgetting one's password, and sharing passwords. Currently, the most common form of system access control in hospitals is the use of unique usernames and confidential passwords [3, 28, 50]. However, this method of access control can lead to concerns about users forgetting passwords or sharing passwords with others, and concerns about hackers using software to determine user passwords and gain unauthorized access to the system [28]. Therefore, other authentication methods have been suggested for the hospital setting.

One alternative access mechanism is smartcards, which are physical cards that users swipe or insert into the EMR system in order to confirm identity of the user [23]. Although these cards are portable and do not require password memorization, there can be problems with the cards potentially being lost, stolen, or damaged [21]. Another alternative access mechanism is the use of biometrics for user identification. Current biometric mechanisms include fingerprint, handprint, or retinal scans, as well as, face geometry technologies [21]. This alternative eliminates the need to memorize passwords or carry a smartcard. However, biometric authentication can be expensive to install and maintain for hospitals, and usability issues can result from environmental temperature, humidity, dirt, and the user's physical condition [18]. In addition, biometric authentication could lead to the users themselves having privacy concerns about the storage and use of their own biometric data [34].

Additionally, the ED staff also used workarounds to improve their workflow efficiencies. This included staff badging each other into restricted areas of the ED, instead of each staff member using his/her own badge. Currently, the most common form of physical access control in hospitals is the use of badges to open doors to restricted areas. This allows the hospital to accurately track the flow of people in restricted sections of the hospital. However, prior literature discusses an alternative to the use of badges for entry – radio frequency identification (RFID) tags.

RFID technology uses electronic chips to store and retrieve data. These chips, or "tags," are attached to objects or people, and the data is read by separate RFID "readers" [19]. The benefits of RFID are that the readers can scan tags while they are in motion and without direct line of sight to the tags [19]. This is beneficial for very busy environments, like hospitals. Within the medical context, RFID is typically used for medication, equipment, and patient tracking, but it has also been considered for staff tracking as well [16, 19].

Tracking hospital staff using RFID helped to improve the workflow of clinicians and quickly locate staff when they were needed for emergencies [16, 19, 53]. In our study, it was a common practice for staff to badge each other into restricted areas of the hospital. Embedding RFID tags into staff badges could be a potential solution for this issue by reducing workflow interruptions (e.g., stopping to find badge to hold to the door sensor) and preventing workarounds that lead to inaccurate records (e.g., badging in other staff). However, hospitals should also consider the negative impacts of using RFID to track staff.

RFID technologies can cause interference with other technologies, have high costs for installing and maintaining infrastructure, and lead to privacy and ethical issues [16, 19, 53]. In one study that explored the staff concerns of RFID tracking, nurses felt that they were "being watched by administration" and that there was increased work because maintaining the technology often fell upon them [16].

Therefore, these alternative technical mechanisms for accessing systems and entering restricted areas provide potential solutions to the policy workarounds described in this study. However, these alternatives raise additional issues regarding cost and privacy concerns. Hospitals will have to weigh the cost-benefit tradeoffs of choosing an alternative to the current technical mechanisms if they chose to explore alternative access control mechanisms.

Policy Design

Although technical design can address some of the tensions between organizational privacy policies and work activities, we also need to start re-thinking organizational privacy policy development and enforcement [14].

The "one-size-fits-all" privacy policy that most organizations have can lead to uneven application throughout the organization [43]. This approach does have the benefit of being much easier to develop, as well as ensure that there is a standard policy throughout the organization. However, these policies are also the ones that are most often violated because they do not account for the variance in work practices across departments. Therefore, organizations may write very general policies that give little guidance or more specific policies that will be often violated because they negatively impact the work practices in the department. Clearly, it is not a simple solution to write departmental-level privacy policies. There are issues with ensuring that departmental policies are in-sync with broader organizational policies, as well as the cost of developing and enforcing multiple different departmental policies. At the same time, this approach may be beneficial in terms of supporting, rather than hindering, departmental work practices.

Another important issue in implementing organizational privacy policies is ensuring that the users (i.e., clinical and non-clinical staff) have effective communication channels to share their feedback on privacy technologies and procedures with IT. One of the challenges that users often

face is that privacy technologies and procedures are usually implemented on the basis of what is required by the privacy policies and do not account for the type of work practices in a department [4, 5, 12, 13, 20, 26]. This is a particular challenge in hospitals that have to comply with a number of legal requirements about ensuring the privacy of health information. Consequently, staff may see the privacy policies as a hindrance to their work. However, improving the communication channels between the two groups could help ensure that problems or issues are readily addressed.

CONCLUSION

An emergency department is a highly collaborative and busy environment where staff, patients, and visitors are all present. This means that there are a variety of challenges to managing information privacy in collaborative settings such as this. Therefore, the ED staff have developed various practices to try to help them manage these challenges.

More broadly, managing privacy is an important but challenging aspect of organizational work. Often times, work practices conflict with organizational policies and staff have to make daily decisions about whether to adjust their work or deviate from the policy. In collaborative environments, this can become even more problematic because of the larger number of people involved.

Through this research, we hope to improve our understanding of privacy practices in collaborative settings. We can then develop organizational policies that better match the on-going work, as well as begin to identify design requirements for the development of privacy-enhancing features that will also support the collaboration.

ACKNOWLEDGEMENTS

The authors are very grateful to the AC and anonymous reviewers for their constructive comments. We would also like to thank the ED staff and hospital CMIO for their willingness to participate in this study, as well as Saijing Zheng for her assistance in preliminary data analysis. This research is supported by the U.S. National Science Foundation under grant IIS-1017247. Any opinions, findings, and conclusions or recommendations expressed herein are those of the researchers and do not necessarily reflect the views of the National Science Foundation.

REFERENCES

1. Ash, J.S., Berg, M., and Coiera, E. Some unintended consequences of information technology in health care: The nature of patient care information system-related errors. *Journal of the American Medical Informatics Association, 11*, 2 (2004), 104-112.
2. Angst, C.M. and Agarwal, R. Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. *MIS Quarterly, 33*, 2 (2009), 339-370.
3. Barrows, R.C. and Clayton, P.D. Privacy, confidentiality, and electronic medical records. *Journal of the American Medical Informatics Association, 3*, 2 (1996), 139-148.
4. Bartsch, S. Exploring twisted paths: Analyzing authorization processes in organizations. In *Proc. Network and System Security*, (2011), 216-223.
5. Bauer, L., Cranor, L.F., Reeder, R.W., Reiter, M.K., and Vaniea, K. Real life challenges in access-control management. In *Proc. CHI 2009*, ACM Press (2009), 899-908.
6. Belanger, F. and Crossler, R.E. Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly, 35*, 4 (2011), 1017-1041.
7. Besmer, A. and Lipford, H.R. Moving beyond untagging: Photo privacy in a tagged world. In *Proc. CHI 2010*, ACM Press (2010), 1563-1572.
8. Bethencourt, J., Sahai, A., and Waters, B. Ciphertext-policy attribute-based encryption. In *Proc. IEEE Symposium on Security and Privacy*, (2007), 321–334.
9. Braun, V. and Clarke, V. Using thematic analysis in psychology. *Qualitative Research in Psychology, 3,* 2 (2006), 77-101.
10. Chen, Y., Nyemba, S., and Malin, B. Detecting anomalous insiders in collaborative information systems. *IEEE Transactions on Dependable and Secure Computing, 9*, 3 (2012), 332-344.
11. Chen, Y. and Xu, H. Privacy management in dynamic groups: Understanding information privacy in medical practices. In *Proc. CSCW 2013*, ACM Press (2013), 541-552.
12. Choi, Y.B., Capitan, K.E., Krause, J.S., and Streeper, M.M. Challenges associated with privacy in health care industry: Implementation of HIPAA and the security rules. *Journal of Medical Systems, 30*, 1 (2006), 57-64.
13. Coiera, E. and Clarke, R. e-Consent: The design and implementation of consumer consent mechanisms in an electronic environment. *Journal of the American Medical Informatics Association, 11*, 2 (2004), 129-140.
14. Culnan, M.J. and Williams, C.C. How ethics can enhance organizational privacy: Lessons from the choicepoint and TJX data breaches. *MIS Quarterly, 33*, 4 (2009), 673-687.
15. Fabbri, D. and LeFevre, K. Explaining accesses to electronic medical records using diagnosis information. *Journal of the American Medical Informatics Association, 20*, 1 (2013), 52-60.
16. Fisher, J.A. and Monahan, T. Tracking the social dimensions of RFID systems in hospitals. *International Journal of Medical Informatics, 77*, 3 (2008), 176-183.
17. Fitzpatrick, G. and Ellingsen, G. A review of 25 years of CSCW research in healthcare: Contributions, challenges, and future agendas. *Journal of CSCW*, (2012), 1-57.

18. Flores Zuniga, A.E., Win, K.T., and Susilo, W. Biometrics for electronic health records. *Journal of Medical Systems, 34*, 5 (2010), 975-983.
19. Fuhrer, P. and Guinard, D. Building a smart hospital using RFID technologies. In *Proc. European Conference on eHealth*, (2006), 131-142.
20. Heckle, R., Lutters, W. G., and Gurzick, D. Network authentication using single sign-on: the challenge of aligning mental models. In *Proc. Computer Human Interaction for Management of Information Technology*, (2008), 6-15.
21. Hewitt, B. Exploring how security features affect the use of electronic health records. *International Journal of Healthcare Technology and Management, 11*, 1 (2010), 31-49.
22. Hoadley, C.M., Xu, H., Lee, J.J., and Rosson, M.B. Privacy as information access and illusory control: The case of the Facebook news feed privacy outcry. *Electronic Commerce Research and Applications, 9*, 4 (2010), 649-664.
23. Hu, J., Chen, H.H., and Hou, T.W. A hybrid public key infrastructure solution (HPKI) for HIPAA privacy/security regulations. *Computer Standards and Interfaces, 32*, 5 (2010), 274–280.
24. Koppel, R., Wetterneck, T., Telles, J.L., and Karsh, B.T. Workarounds to barcode medication administration systems: Their occurrences, causes, and threats to patient safety. *Journal of the American Medical Informatics Association, 15*, 4 (2008), 408-423.
25. Liu, C. and Arnett, K.P. Raising a red flag on global WWW privacy policies. *Journal of Computer Information Systems, 43*, 1 (2002), 117-127.
26. Lovis, C., Spahni, S., Cassoni, N., and Geissbuhler, A. Comprehensive management of the access to the electronic patient record: Towards trans-institutional networks. *International Journal of Medical Informatics, 76*, 5 (2007), 466-470.
27. Mandl, K.D., Szolovits, P., and Kohane, I.S. Public standards and patients' control: How to keep electronic medical records accessible but private. *British Medical Journal, 322*, 7281 (2001), 283-287.
28. Medlin, B.D. and Romaniello, A. An investigative study: Health care workers as security threat suppliers. *Journal of Information Privacy and Security, 3*, 1 (2007), 30-46.
29. Murphy, A.R., Reddy, M.C., Xu, H., and Ringel, B. Exploring collaborative privacy practices. In *Proc. CHI 2011 Workshop "Privacy for a Networked World: Bridging Theory and Design,"* ACM Press (2011).
30. Narayan, S., Gagne, M., and Safavi-Naini, R. Privacy preserving EHR system using attribute-based infrastructure. In *Proc. ACM 2010 Workshop "Cloud Computing Security,"* ACM Press (2010), 47-52.
31. Palen, L. and Dourish, P. Unpacking "privacy" for a networked world. In *Proc. CHI 2003*, ACM Press (2003), 129–136.
32. Parks, R., Chu, C. H., and Xu, H. Healthcare information privacy research: Issues, gaps and what next? In *Proc. 2011 Americas Conference on Information Systems*, (2011).
33. Patil, S. and Kobsa, A. Privacy in collaboration: Managing impression. In *Proc. 2005 International Conference on Online Communities and Social Computing*, (2005).
34. Prabhakar, S., Pankanti, S., and Jain, A.K. Biometric recognition: Security and privacy concerns. *IEEE Journal of Security & Privacy, 1*, 2 (2003), 33-42.
35. Randell, R., Wilson, S., Woodward, P. and Galliers, J.R. The ConStratO model of handover: A tool to support technology design and evaluation. *Behaviour & Information Technology, 30*, 4 (2011), 489-498.
36. Reddy, M. and Dourish, P. A finger on the pulse: Temporal rhythms and information seeking in medical work. In *Proc. CSCW 2002*, ACM Press (2002), 344-353.
37. Salomon, R.M., Blackford, J.U., Rosenbloom, S.T., Seidel, S., Clayton, E.W., Dilts, D.M., and Finder, S.G. Openness of patients' reporting with use of electronic records: Psychiatric clinicians' views. *Journal of the American Medical Informatics Association, 17*, 1 (2010), 54-60.
38. Smith, H.J. Privacy policies and practices: Inside the organizational maze. *Communications of the ACM, 36*, 12 (1993), 105-122.
39. Smith, H. J., Dinev, T., and Xu, H. Information privacy research: An interdisciplinary review, *MIS Quarterly, 35*, 4 (2011), 989-1015.
40. Son, J.Y. and Kim, S.S. Internet users' information privacy-protective responses: A taxonomy and a nomological model. *MIS Quarterly, 32*, 3 (2008), 503-529.
41. Stutzman, F. and Kramer-Duffield, J. Friends only: Examining a privacy-enhancing behavior in Facebook. In *Proc. CHI 2010*, ACM Press (2010), 1553-1562.
42. Squicciarini, A.C., Xu, H., and Zhang, X. CoPE: Enabling collaborative privacy management in online social networks. *Journal of the American Society for Information Science and Technology, 62*, 3 (2010), 521-534.
43. Turner, E.C. and Dasgupta, S. Privacy on the web: An examination of user's concerns, technology, and implications for business organizations and individuals. *Information Systems Management, 20*, 1 (2003), 8-18.
44. U.S. Department of Health and Human Services. (2013). "Breaches Affecting 500 or More Individuals." Retrieved from:

http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html.

45. U.S. Department of Health and Human Services. (2013). "Health Information Privacy." Retrieved from: http://www.hhs.gov/ocr/privacy/.
46. U.S. Department of Health and Human Services. (2013). "HITECH Act Enforcement Interim Final Rule." Retrieved from: http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html.
47. U.S. Government. (2013). "American Recovery and Reinvestment Act of 2009". Retrieved from: http://www.recovery.gov/About/Pages/The_Act.aspx.
48. Vogelsmeier, A.A., Halbesleben, J.R.B., and Scott-Cawiezell, J.R. Technology implementation and workarounds in the nursing home. *Journal of the American Medical Informatics Association, 15*, 1 (2008), 114-119.
49. Wears, R. L., Perry, S. J., Wilson, S., Galliers, J., and Fone, J. Emergency department status boards: User-evolved artefacts for inter-and intra-group coordination. *Cognition, Technology & Work, 9*, 3 (2007), 163-170.
50. Win, K.T. A review of security of electronic health records. *Health Information Management, 34*, 1 (2005), 13-18.
51. Xu, H., Dinev, T., Smith, H.J., and Hart, P. Examining the formation of individual's information privacy concerns: Toward an integrative view. In *Proc. International Conference on Information Systems*, (2008).
52. Xu, H., Teo, H.H., Tan, B.C.Y., and Agarwal, R. The role of push-pull technology in privacy calculus: The case of location-based services. *Journal of Management Information Systems, 26*, 3 (2009), 137-176.
53. Yao, W., Chu, C.H., and Li, Z. The use of RFID in healthcare: Benefits and barriers. In *Proc. 2010 IEEE International Conference on RFID Technology and Applications*, (2010), 128-134.