Privacy Management in Dynamic Groups: Understanding Information Privacy in Medical Practices

Yunan Chen
University of California, Irvine
5066 Bren Hall, Irvine, CA, 92697
yunanc@ics.uci.edu

Heng Xu
The Pennsylvania State University
316H IST Building, University Park, PA 16802
hxu@ist.psu.edu

ABSTRACT
Recent wide adoption of Electronic Medical Record (EMR) systems provides health practitioners with easy access to patient private information. However, there is a dilemma between the easy access to patient information and the potential privacy infringement brought by such easy access. This paper elaborates three types of group dynamics that identify challenges of privacy management in medical practices: team members, temporal involvement, and different levels of information sensitivity. Drawing on the theory of *contextual integrity,* this work identifies the appropriate actors, information access, and information transmission principles for understanding the norms of information flows. The findings of the study shed lights on the design insights that privacy enhancing features should be appropriately aligned with the dynamic group behaviors of medical practices.

Keywords
Electronic Medical Record (EMR); access control; information privacy; privacy-by-redesign; patient care teams; group dynamics.

ACM Classification Keywords
K.4.1 [Public Policy Issues]: Privacy, H.0 [information systems], K.4.3 [organizational impacts], J3.Life and Medical Sciences: Health, Medical Information Systems.

INTRODUCTION
As medical practices speed into the digital age, privacy has become an ever-present challenge. One particular challenge is how to prevent inappropriate access, use, and diffusion of private patient information in Electronic Medical Record (EMR) systems. EMR is an organization-wide IT infrastructure that contains patients' entire medical records assembled from various sources. It is projected that the adoption of EMR systems will exceed 70% in U.S. healthcare organizations by 2019 [38]. EMR offers a magnitude of benefits to future medical practices, *e.g.* accurate diagnosis, error prevention, easy communication, and patient care -- all relying on the improved accessibility of patient information. However, EMR's anticipated value is potentially discounted because of concerns involving highly personal and sensitive nature of healthcare data and associated privacy.

To protect patients' privacy rights, prior research advocated implementing privacy safeguards to reduce privacy concerns and protect sensitive health information [1]. Nevertheless, these privacy safeguards do not seem effective [36] and privacy breaches frequently occur. Since 2005, the Privacy Rights Clearinghouse has reported over 22 million healthcare-related privacy breaches [34]. Situations where personal health information is stolen or disclosed without authorization have been widely discussed in the media and have raised broad awareness about the digitization and use of personal health information in medical practice. For example, it was reported in 2011 that employees at a University Medical Center in Tucson inappropriately accessed the U.S. Rep. Gabrielle Giffords' medical records through the hospital-wide EMR system, following the shooting rampage at a local supermarket five days earlier [41]. The three clinical support staff members and a contracted nurse were soon fired due to the violation of patient privacy, since none of them were involved in the treatment or care of Giffords.

According to the privacy rules of Health Insurance Portability and Accountability Act (HIPAA) in the United States, individuals need to have a legitimate reason to legally access a patient's medical records, such as participating in a patient's treatment, care, or billing. Those who work in the same health organization, but are not involved in a patient's case, have no right to access. In the Giffords' case of privacy breach, the hospital officially stated that, "UMC uses sophisticated technology to help prevent and detect inappropriate access to patient information [41]." Technologies, such as access controls implemented in EMR systems facilitate the detection of inappropriate access to patient information. However, these cases indicate that many current EMR systems may not prevent inappropriate access before it occurs. With the wide adoption of EMR systems, insider abuse of personal health information is by no means a rare case. What is left to be solved is -- *how can EMR systems help prevent such privacy breach from happening?*

CSCW '13, February 23–27, 2013, San Antonio, Texas, USA.

Even though privacy management[1] has been well studied, prior studies often focused on *organization-wide* privacy practices, i.e., establishing preventative measures such as organizational policies, privacy enhancing technologies, and administrative processes [31], to alleviate concerns for the privacy of the organizations' customers. Nevertheless, these organizational-level privacy practices may not align with employees' actual information behaviors [5, 21], especially in a dynamic and collaborative environment such as healthcare, where teamwork is crucial to the execution of patient care tasks. From this perspective, largely missing from current understandings of privacy management are studies examining *group* level privacy concerns, i.e., the collective concerns that group members have regarding the privacy of information to which the group possesses and has access in an organization [6].

This void in extant privacy literature has also been identified by Murphy et al. [25], who highlights the need for studying group-level privacy practices in the healthcare setting. As noted by Murphy et al. [25], sensitive health data are often co-managed by different groups of medical employees who collectively share, use, and communicate patients' medical records in their medical practices. Therefore, the accuracy and confidentiality of a patient's medical records is the joint responsibilities of multiple medical teams who provide care to that patient.

Drawing insights from three recent ethnographic studies in the use of EMR systems at various medical settings, this paper identifies three forms of group dynamics that are particularly challenging in designing privacy safeguards. We believe that this work contributes to the privacy research in several important ways. First, this research provides new theoretical insights into understanding privacy management by studying group dynamics in complex medical practices. Second, Smith et al. [37] call for more qualitative research to study privacy management, and the challenge is that studies in organizational settings "*are necessarily more complex and less conducive to 'quick' data collection techniques such as written and online surveys*" (p. 1006). In response to this challenge, this research aims to understand privacy management in health organizations through ethnographic field studies. Third, Fitzpatrick [17] has noted it is critical to emphasize policy driven innovations. In particular, she mentioned, "*CSCW research will not have significant impact unless it engages in such advocacy alongside undertaking studies* [17]." In line with this thought, the insights obtained through our field studies are likely to contribute to both the technical development, as well as the privacy policy design in similar collaborative and dynamic working environments.

[1] In this research, we focus on privacy management problems resulting from information practices in terms of collection, use, security, and distribution of personal information [13]. Consistent with Culnan and Williams [13], we define security as one aspect of privacy and argue that privacy includes more than security. According to Culnan and Williams ([13], p.675), "privacy is broader and encompasses permission and use of personal information. Privacy is difficult to achieve without security. However, organizations can successfully secure the personal information in their databases but still make bad decisions about subsequent use and distribution of personal information, resulting in a privacy problem."

RELATED WORK

Collaborative Work and Privacy Management

The collaborative nature of medical work has been studied extensively in the CSCW literature, with a focus on understanding work behaviors and system use in real health contexts [17]. This is because the success of patient care often relies upon effective team collaboration, and collaborative work behaviors cannot be obtained without studying work behaviors *in situ*. Compared with other static collaborative settings, collaboration in the medical field is characterized as dynamic and information-rich [7, 24, 35]. As such, many studies have been conducted to examine complex medical practices *in situ*, in the hopes of gaining insight to inform the design of systems deployed in these settings. Various and important aspects of group-level work practice have been discussed in prior literature, including temporal coordination [35], spatiality and mobility [3], and formality of artifacts [10]. In particular, one study shows that groups are dynamically formed and evolve rapidly *in situ* [23]. Collectively, this body of literature indicates the needs of grounding design in the group dynamics of medical practices, since the lack of consideration of collaborative work often leads to system failures in organizations [19].

As opposed to group-based work practices studied in the CSCW field, prior privacy studies mainly consider privacy management at the organizational level, and fail to recognize the need for privacy protection at the group level. This void in extant privacy research has been identified by a recent interdisciplinary literature review [37] that highlights the need for more privacy management research at the team or small group level, as well as by online privacy research in the HCI field, *e.g.* [29]. To provide a richer conceptual description of privacy management, this study is targeted to this under-researched level of analysis.

Effectiveness of Privacy Safeguards in Healthcare

There is a growing body of privacy research examining organizational responses to privacy threats in the context of healthcare [15, 30]. Parks et al. [31] suggest that health organizations respond to privacy threats through a combination of technical and behavioral means. Technical safeguards such as access control [33], anonymization [28] and encryption [22] have been studied in prior literature. Nevertheless, implementing these technical safeguards in medical practices may impede the operational activities of medical employees [2]. In term of behavioral means of privacy safeguards, prior research has investigated the impact of training, promoting, and educating medical professionals about privacy and security awareness [32]. In the pursuit of privacy compliance, organizations implement these privacy safeguards that may change medical workers'

operational workflow [12]. As a result, users may not always react positively to implemented changes, especially when privacy safeguards disrupt their work routines [8]. Therefore, establishing safeguards in harmony with the "actual day-to-day procedures" remains one of the major challenges of healthcare organizations [11].

THEORETICAL FOUNDATION

To better understand privacy expectations and the norms of the transmission of personal information in a given context, the theory of *contextual integrity* [26, 27] because it theorizes the **context-relative informational norms** which "*regulate the flow of information of certain types about an information subject from one actor (acting in a particular capacity, or role) to another or others (acting in a particular capacity, or role) according to particular transmission principles*" (p.141). Specifically, context-relative information norms are characterized by four key parameters: *contexts, actors, attributes, and transmission principles* [27]. Among these parameters, *contexts* are the circumstances in which the information flows are situated in; *actors* including information recipient (who receives information), information subject (whom the information is about), and information sender (who transmits the information)*; attributes* are defined as the types of information in the information flow*; transmission principles* are the constraints to the information flow from one party to another in a given context.

Applying Nissenbaum's framework to understand the informational norms in medical practices, we consider the *context* as the circumstances in which an act of information handling is prescribed by medical employees. In this research, the *actors* we concern about are medical employees who write, share, and communicate patient's information (information senders and recipients); while patients (information subjects) are not examined in this study. In a healthcare context, there are different *attributes* or types of information being used and distributed in EMR systems, such as patients' diagnose information, contact information, medical histories and etc. In U.S., the *transmission principles* that govern the flow of information is the HIPAA regulation, which requires that accessing protected health information follow the minimum necessary rule. Under the general minimum necessary rule, medical employees have to have a legitimate reason, such as participating in a patient's treatment, care, or payment process, to access a patient's medical records.

In addition, the norm of **appropriateness** is a distinctive notion from the theory of contextual integrity [26]. Appropriateness dictates what personal information is appropriate to handle or reveal in a given context wherein data practices and actions are performed [26]. In medical practices, we interpret the norms of appropriateness as a set of norms as to whether the information accessed by a medical employee is considered appropriate to the role s/he serves, and the specific context at the moment of access. To that end, although the healthcare industry has established legislative efforts in HIPAA, aligning norms in harmony with actual dynamic work practices remains one major challenge. In particular, the normative guidance provided by HIPAA regulation does not define the appropriate levels of privacy protection corresponding to the types of personal information and the specific situation under which the information is accessed and revealed.

Therefore, understanding the informational norms in medical practices are no easy tasks, since norms are not static. Instead, they are dynamically changing when the parameters of informational norms change. New norms are emerged and have to be considered when information distribution is passed to a new recipient, encountered under a new situation, or with new constraints. In this work, we aim to: (a) understand the informational norms in medical practices, and (b) investigate the extent to which privacy safeguards designed in current EMR systems may align or misalign with the contextual informational norms in medical practices.

In this paper, we base our argument on the theory of contextual integrity [26] because it ties privacy protection to *"norms of specific contexts, demanding that information gathering and dissemination be appropriate to that context and obey the governing norms of distribution within it*" (p.101). In other words, the informational norms should be engrained into medical teams' daily data practices to determine *who* can access or distribute *what kinds of information under what situations and constraints*. Consequently, privacy protection mechanisms should be designed and enforced at an appropriate level in order to facilitate appropriate information flow and to establish norms of appropriate information use in a specific situation.

METHODOLOGY

As Barkhuus [4] points out, in the privacy literature, "*it is rare to see studies that implemented real systems with real data sharing or which [are] used in-situ data*." To respond to such a compelling call for "*contextually-grounded research that explores privacy issues in the wild* [4]," we obtained data from qualitative field observations to study the group-level privacy practices mediated through the EMR systems-in-use and to understand the norms of information flows that challenge the privacy management in actual clinical work practices. The research context is the patient care conducted in health organizations. Users who have the right to access the patient data held in EMR systems are doctors, nurses, case managers, billing personnel, and lab technicians -- those who actually engage in patient cases in the medical setting. Other users, such as researchers who access patient records for chart review studies, or health consumers, such as patients and their family members, will not be discussed in this study.

The data reported in this paper were drawn from three recent qualitative studies (see Table 1) examining the use of EMR systems in different health settings. Although these

studies were originally designed and carried out for studying the use of EMR systems in diverse clinical settings, the data obtained from these field observations give us an opportunity to study the norms of information flow and the EMR systems-in-use at our field sites. It should be noted that this study does not intend to reveal privacy infringements, nor to criticize the design of privacy enhancing features in the EMR systems we studied. Instead, our intention is to understand the nature of group dynamics in medical practices in order to examine the extent to which the design of EMR systems effectively supports information flow in medical teams' work practices.

Site	Organizational Context	EMR
ED	Regional healthcare center	System A
Clinic 1	Technology pilot site for a nationwide health system	System A
Clinic 2	Free Clinic serving for the poor	System B

Table 1: Summary of the ethnographic studies

Studies

Ethnographic study methods, including field observations, in-depth interviews, and informal probes, were used in all three studies[2]. Specifically, the field observations allowed us to uncover nuanced information behaviors in the real working environments. Formal and informal interviews were used to gather medical employees' perceptions, attitudes and preferences about technology-in-use.

Emergency Department (ED): Work Efficiency & EMR Use

The first study was conducted in an ED affiliated with a large regional hospital. ED work practices and workflows are extremely complex because of its diverse patient situations and their urgent care needs. At the time of this study, a full-functioning EMR system had already been implemented in the ED. However, the use of the newly introduced EMR system was coupled with decreased work efficiency and complicated workflow. The ED study was set forth to examine ED workflow and efficiency with EMR use accordingly.

A total of 120 hours of field observations were conducted during a period of three months. Each observation session lasted for 4-5 hours, during which brief notes were jotted down using pen and paper, and detailed notes were transcribed after the observation sessions finished. Brief informal interviews were probed with ED staff members during and after each observation session. During the study, we observed the general activities in the ED, shadowed ED employees, asked questions, tracked critical incidents and followed various patient cases. Our observations were able to cover most of the ED employees during work, either briefly in the public area or through close shadowing. The observations started with the overall activities on the ED floor. We followed 6 entire patients' treatment processes, shadowed 5 ED doctors, 4 triage nurses, 5 room nurses, and 2 case managers. In addition, we observed other employees, such as receptionists, billing personnel, technicians, social workers, and specialists.

Clinic 1: EMR Usages in an Outpatient Clinic

The second study aims to examine the use of the EMR system in an outpatient clinic affiliated with a large healthcare organization. Unlike the ED setting, medical conditions being treated in an outpatient clinic are usually not urgent, but are oriented towards disease management and prevention. The main purpose of the Clinic 1 study was to understand the impact of the EMR system on patient-provider interactions during routine medical visits. The EMR system at the field site had been in use since 2008 and was integrated as part of routine work practices. We shadowed 5 out of the 9 primary care physicians in the clinic, with a total of 140 patient visits during the study. Observation data on doctors were primarily collected in the exam-rooms and physicians' offices. In addition, we also observed other medical and administrative staff members, including medical assistants, front desk personnel, team leads, and schedulers to obtain a broader understanding of work practices. In total, we collected 180 hours of field observations over 6 months. In the exam-room, when patients were present, we passively stayed behind-the-scenes, writing down notes related to technology-use and clinicians' behaviors. Observations in the offices were conducted through a think-aloud manner, where we sat at the back of the office observing physicians' behaviors while the doctors explained their activities and the reasons behind the tasks they were doing. Data from the informal interviews and observations were noted using pen and paper on-site, and then transcribed in more detail later.

Clinic 2: EMR Rollout in a Free Clinic

The third study was an examination of the rollout of an EMR system at a free outpatient clinic primarily serving for low-income and homeless population. Patients in this clinic normally do not have health insurance, and many even require further social services. Most of the employees at this free clinic are those who also hold jobs at other health organizations and are volunteering at the clinic temporarily. The unique practices of this clinic are useful in studying how the EMR system is used in a volunteer dominant working environment. Approximately 40 hours of field observation, both before and after the EMR rollout, were conducted. Field observation data were collected in the same way as we described in the previous two studies. In addition, we also conducted in-depth interviews with 14 clinic staff members after the EMR rollout to gather their opinions regarding the new system. Interviewees included medical directors, nurses, medical assistants, medical record coordinators, as well as volunteers in the free clinic.

[2] The human subject research approvals were obtained in all the field sites prior to the studies.

Interviews lasted between 30-45 minutes, and were audio-recorded. One medical director was also interviewed before the EMR rollout in order to understand the process of the system's deployment. Together, a total of 15 interviews were collected, which include most paid employees and selected volunteers in this free clinic.

Data Analysis

Although these ethnographic studies were not designed to specifically study privacy managements, the deep understandings of how work practices are performed during real patient care inspire one central question in privacy management – *who uses what types of information according to what transmission principles?* Answering this question is crucial to the understanding of how privacy features should be designed to align with actual work processes. With this goal in mind, we first reviewed observation notes and interview transcripts, and extracted data that were relevant to the use of patient information in medical practices, with specifically attention paid to the users (actors), the types of information (attributes) as well as the ways how information is shared within teams (transmission principles). The extracted notes were then analyzed using grounded theory approach [18] to uncover behaviors of information practices across all three field sites. We focused on the differences between how information is accessed and used in actual patient care, and how such information is stored and protected in the systems. The initial information usage patterns were coded, with an open coding approach to identify new concepts from the data. This process was followed by an iterative process of collapsing our first round of codes into conceptually distinct themes. Through this coding process, we identified team members, temporality, and information sensitivity as the three main norms for patient information flow in medical practices.

FINDINGS

In this section, we describe the information accessibility afforded by EMR systems, and the privacy control mechanisms designed in EMR systems from our field sites. We then discuss three forms of group dynamics identified through field observations to highlight the unique challenges of privacy management in medical practices. We argue that these group dynamics are embedded in the norms of appropriateness and information flow, as they reveal the ways in which privacy safeguards designed in current EMR systems may or may not align with the norms of appropriateness and information flow.

Better Accessibility Afforded by EMR Systems

Accessing patient information online anywhere and anytime is a major benefit that EMR systems intend to bring to medical practices. With these centralized systems, there is no longer one physical copy of a medical chart that can be used by only one user at a single location; instead, multiple clinicians can simultaneously read, review and document in the same electronic record from their work settings or other offsite locations (see Figure 1). This enhanced accessibility was illustrated through the ubiquitously placed EMR systems at all three field sites. At the ED site, desktop terminals to access the EMRs were available almost everywhere, at patients' bedsides, in hallways, and at doctors' desks. Similarly, in the outpatient clinics, EMR systems were available in exam-rooms, doctors' private offices, front desks, and in the medical assistants' desks located in the hallways. In addition, most doctors can access the EMRs from outside clinical environments (e.g., when they work from home).

Figure 1: ED doctors checking (left) and documenting (right) in the shared EMR system.

The improved accessibility of the systems enables the EMRs to mediate various collaborative practices among different medical team members synchronously. For instance, in the ED setting, when a nurse updates a patient's progress in the EMR system at a patient's bedside, the doctor, who is in charge of the patient, can view the updated note immediately from his end. After orders are prescribed in the EMR system, nurses and technicians can be notified when they logon to the system. Likewise, primary care physicians can oversee patients' situations by reading the medical notes authored by other specialists. These observations demonstrate that EMR systems are not only record-keeping tools, but also universal infrastructures that mediate various forms of collaboration and communication that are often distributed across time and location in medical settings.

Privacy Enhancing Features in EMR Systems

Consistent with prior research that identifies both technical and behavioral means to assure health privacy [30], we also observed both behavioral and technical safeguards in our field sites. In terms of behavioral safeguards, medical employees are expected to follow the privacy guidelines set by health organizations. As we witnessed at our field sites, summaries of HIPAA privacy rules are posted on flyers or are even set as the background on computer screens to remind employees that, without a legitimate reason, they should not access patient medical records. In terms of technical safeguards, the EMR systems we studied are designed with privacy protective features that allow only authorized users to access the patient information stored in the system. Medical employees working in a given healthcare organization are provided with user names and passwords in order to access the organization-wide EMR. This password protection mechanism is designed to prevent outsiders from accessing patient records.

Within each health organization we studied, the EMR system was initially designed by a vendor company and was then customized based on the organization's work routine, operational procedures, local considerations, as well as patient care needs. Consequently, the privacy enhancing features in these systems were also customized by each organization. Nevertheless, we observed a universal access control mechanism through an *all-or-nothing* approach, i.e., employees were either allowed or denied access to patient information in the system. Such a static approach often fails to recognize the specific roles employees from different departments serve in different medical practices.

At our field sites, there was also a lack of differentiated access for different types of medical groups. Consequently, privacy features were rarely enacted at the *group* level in the system to prevent and detect illegitimate access among multiple medical teams. The need for access control at the group level arises due to the inability to monitor all team members and their privacy practices. On one hand, medical teams collaborate on various medical tasks and make decisions based on their gathering, accessing, analyzing, and sharing of patients' medical records. On the other hand, the effectiveness of these collaborative medical practices impact whether or not the privacy and confidentiality of the records will be maintained.

In what follows we describe three types of group dynamics that are unique to medical practice and discuss why group-level privacy protection is a particularly challenging issue to tackle.

Group Dynamics in Medical practices

As illustrated in the *illness trajectory* concept, the health management of a patient contains the entire course of a disease and the associated work in its different stages and phases [39]. For instance, a diabetic patient's trajectory work includes the treatments s/he receives from all emergency, routine, and medical specialists, *e.g.* podiatrist visits in different stages and times of the overall diabetic care. Health practitioners involved in patient cases are all reliant on the use of the private information documented in the medical records to make informed decisions and to continue with follow-up treatments. In this sense, being users of shared, yet private, patient information is the basis for team collaboration in healthcare, and such collaboration is often across temporal and departmental boundaries. Nevertheless, the highly dynamic nature of medical teams makes it difficult to define the boundaries of groups in medical practice, and consequently, makes group-level privacy management more difficult to implement.

In this section, we outline three types of group dynamics found in medical practice, and use cases drawn from our ethnographic studies to illustrate the question of *who uses what types of information according to what transmission principles*. The three types of group dynamics are:

- The constantly changing group members,
- The dynamic life spans of team formation, and,
- The different levels of information sensitivity.

1. Dynamic Team Members

Different from other collaborative teams which are more static (e.g. those in regular office settings), patient care teams are dynamically formed *in situ* with distinctly different team members. Because of this, it is not easy to predefine who will be in which patient team before a patient's arrival. In many cases, even the roles required for a patient's care cannot be determined beforehand and are decided *in situ,* when the patient has been presented. This unpredictability in determining patient care team members adds to the challenges of defining and designing group-based privacy control features. In this section, we describe the patient treatment processes at our sites to demonstrate the dynamic nature of medical teams.

Group dynamics are a salient issue in ED settings since patients in the ED present a wide range of medical situations with varied urgencies. Teams can only be formed when a patient has arrived on site, and the teams continue evolving when new progress, new orders and new situations occur. To illustrate the dynamics of team members, here is a typical patient treatment drawn from field observations conducted in the ED.

When a patient walks into the ED, s/he first checks in at the front desk, where a nurse and a receptionist ask for the chief compliant and measure the patient's vital signs. Then the patient is called into the triage for a more detailed assessment. Triage assessment determines the severity of the patient case, and assigns the patient to a specific room according to the severity of the situation and doctor's expertise, e.g. adult or pediatric care; the main ED or the urgent care unit. Once the patient is assigned to a room, the nurse, who is in charge, starts monitoring his/her situation. The room nurse then conducts a more detailed assessment and marks the case as ready in the EMR system. On the other end of the ED, doctors constantly browse through newly admitted patients in the EMR, and pick patients based on their expertise and availability. The doctor sees patients in their rooms, and return to his/her desk to prescribe medications, or lab orders. After receiving the orders, the room nurse and technicians work on them respectively. Lastly, after the patient's situation is stabilized in the ED, a case manager will start preparing the transfer or discharge paperwork for the patient.

In the scenario described above, an ED patient care team usually consists of a receptionist, a triage nurse, a room nurse, an ED doctor and a case manager, as well as technicians and other professionals, during the few hours of the patient's stay. Among these different roles, the doctor and the room nurse act as the *core team members* since these roles are required for the patient's entire stay, and the others serve as *peripheral members* since they only join the team as needed. Other more complicated patient cases often have to deal with situations like discussions with doctors in

other departments or hospitals; treating urgent, traumatic cases; and managing patients with other social and financial needs. These complicated situations, as we have seen in the study, involve various specialists, primary care physicians, admission doctors and social workers, who often do not work in the ED.

The challenge of dynamic team members also exists in outpatient care, especially in clinics that have multiple physicians. As seen in the Clinic 1 study, doctors and medical assistants work in pairs to treat patients, yet doctors do not always collaborate with the same assistant. In fact, our observations with the two schedulers at Clinic 1 show that the full schedule of each day was usually planned every morning at 7 am – only one hour before the operation of the clinic began. In addition, there were different medical assistants who covered lunch breaks and took over during shift changes. For instance, we frequently saw medical assistants handoff their job in the middle of a patient case at 5pm when one assistant had to leave and the other arrived at work, while doctor had to stay longer to finish all the scheduled appointments. Further, the different shift changes and availabilities among random radiology technicians, nurses, and team leads also complicated what was otherwise relatively routine outpatient care. In these cases, although the doctor of each patient was scheduled in advance, the rest of the patient care team was formed dynamically *in situ*.

In addition to the group dynamics of a patient care team, each medical employee often participates in multiple care teams that all have distinctly unique configurations simultaneously. As our observation shows, an ED nurse takes care of 4-5 patients, and an ED doctor is usually in charge of 8-10 patients at a time. We also observed that nurses in the ED are assigned to patients based on rooms, while doctors are assigned to patients based on their expertise and availabilities. Thus, teams generally do not have the same doctor or nurse. Similarly, a family doctor may work with many different medical assistants, nurses, specialists and technicians for the patients in his/her panel. Together, such cross-team involvement forms an intricate care network where the boundaries of the teams are difficult to define (Figure 2).

In summary, the challenge of defining the scope of a patient care team in medical work is tri-folded. First, the roles of a patient care team are defined as the treatment evolves *in situ*; second, the specific person who works in these roles are dependent on the situation at the moment; and third, medical employees are always involved in multiple patient care teams, and each team has its own team members. The dynamic nature of scoping exact team members presents great challenges for defining which individuals constitute a patient care team, and who should be granted access to a patient's records in the EMR system.

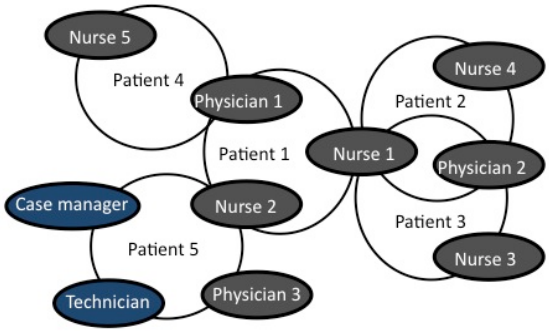

Figure 2: Team Dynamics in Medical Practices. Each patient care team constitutes both core team members (in black) and peripheral members (in blue). Meanwhile, cross-team involvement is a common practice in health settings.

2. Diverse Life Span of Teams

In addition to dynamic team members, the duration of teams also vary dramatically depending on each patient situation. As we described earlier, when a patient arrives at a health setting, the patient care team is formed dynamically on site. Similarly, when the patient care work is completed, the patient care team disassembles, and members of the team take on other patient cases to continue their work. Since a patient care team is only temporarily formed, access to private patient information should be granted accordingly in a time-sensitive manner. Thus, the temporal dimension becomes another concern that adds to group dynamics in medical practice. Temporality is a rather complicated factor to measure in healthcare group dynamics. In this section, we illustrate two aspects of temporality: 1) the dynamic life span of teams in medical practice; and 2) the volatile time span for core and peripheral team members.

The two types of medical teams we studied at our field sites introduced us to diverse forms of team durations. The nature of ED care determines that patients do not visit the department on a routine basis. The actual time span of each ED visit is dependent on the severity of the patient case, the psychological responses to treatment, and other logistical factors. Our observations showed that an ED visit could be as short as 2-3 hours or as long as 1-2 days. In contrast, patients often visit their family doctors routinely over a long period of time, *e.g.* on many occasions we shadowed patients who had been with a doctor for over multiple years. Visits to outpatient clinics usually have a prescheduled and fixed duration: patients schedule an appointment for 20-30 minutes in advance; the core team member, usually the primary care doctor, stays in the patient team longitudinally, regardless of changing medical assistants, specialists, nurses and technicians. In this sense, the patient care team in outpatient care can be viewed as a long-term oriented team with a fixed core and ever-changing peripheral members. Long and short term team durations often co-exist in a patient overall health trajectory, making

it a challenging task to define the duration of team access, and consequently, difficult to define the temporal dimension of group-level access to patient information.

Another group dynamic lies in the volatile time involvement of the patient care team members, especially for core and peripheral members. As stated by Strauss [39], a doctor and nurse are required to cover therapeutic and monitoring levels of patient care throughout an entire hospital stay, but other team members just treat the patient briefly. Cases such as this were observed in the ED, where a doctor and a room nurse, who represent the core team members, stay in the team from a patient's arrival till discharge. Other peripheral members only join the team for a short period of time. In our study, we found that a technician only participates in patient care during the time of taking an EKG, a case manager only joins the team after the decision for hospital admission has been made, and a receptionist deals with appointment scheduling and registration. Although a family doctor sees a patient for years, constantly there are different medical assistants, nurses and specialists who join and leave the patient care team. Granting core and peripheral members access to private patient information for the same duration can be problematic since those people should not access the records after they leave the care team.

In addition, the access and use of medical records may occur both before and after the formation of medical teams. Although it is expected that doctors will review patient information, conduct medical consultations, and document relevant information in the EMR at the of a visit, their heavy workload and working styles often prevent them from doing so. For instance, some doctors we studied in Clinic 1 prefer to review patients' charts one or two days prior to their visits, and most doctors only have time to complete their documentations hours after the patients' visits have been completed. On many occasions, we observed outpatient doctors chart in patient records during lunch breaks, evenings or early morning the next day. Many of the ED doctors we shadowed also hold patient information till the end of 12-hour shifts and document them in the system all at once, since only then do they have the uninterrupted time to write long progress notes. This prolonged working time, which exceeds the actual patient care time, also complicates the duration of the chart using time, and consequently challenges access-control from the perspective of temporality.

The prolonged charting time often makes doctors open patient charts longer than the actual medical visit period. One outpatient doctor we studied even complained that she got warning messages from the IT department since she kept the charts open for too long. This observation suggests that privacy policies and features have to be compatible with the temporal dynamics of patient care teams, instead of implementing a one-size-fits-all policy for the use of medical charts.

In summary, the dynamic life span of medical teams also affects group-level privacy practices. What we have seen at field sites suggests that both the durations of patient care teams, and the length of the team members' involvement, vary on a case-by-case basis. Designing a group-based access control that aligns with the dynamic and volatile temporal aspect of team formation is a critical, yet challenging, issue to consider in protecting patient privacy at the group level.

3. Different Levels of Information Sensitivity

Last, the extent to which a team member should be granted access to patient information also varies greatly. Patient records in an EMR system contain a broad range of information from a person's name, address, date of birth and phone numbers to diagnoses, medications, radiology images and medical and social histories. These records may also cover information regarding a wide range of patient diseases, from the common cold to more sensitive mental and psychological disorders. The lengthy personal and medical data accumulated over time are all packed into one medical record in the centralized system. With the diverse and ever-changing users of the records, granting everyone the same amount of access without differentiating sensitivity levels can be problematic. In this section, we use cases collected from the two outpatient clinic studies to exemplify the need for having layered access control for different types of information with different levels of sensitivity in a single medical chart. These cases point to the need for granting different levels of privacy control for team members who serve different roles, indicating that patient information has different levels of sensitivity.

In Clinic 1, we studied the use of the EMR system among primary care physicians. The major role of primary care physicians is to oversee a patient's whole spectrum of health and to serve as a gatekeeper for other emerging and specialized illnesses. Because of this, physicians always read and review medical notes authored by other healthcare providers, as they are obligated to know why their patients went to an ED prior to their current medical visit or what the progress has been with other specialists and therapists in between a patient's two routine visits. Having easy access to a patient's entire medical record has greatly benefited primary care physicians. However, at Clinic 1, there was a privacy control feature being implemented to limit primary care physicians from accessing patients' mental health records. Frequently during observations we saw primary care physicians become frustrated about not being able to view the notes made in the system by psychiatrists and psychologists. Physicians can see the medications a psychiatrist prescribed, but cannot access the medical documentation associated with the orders. There was one case observed in the study, when a physician found out that her patient had depression, and had been consulting with a psychiatrist in the same healthcare organization for more than a year. The doctor was shocked and frustrated that she had not known, since she would have otherwise prescribed

medications differently. In this case, when a mental illness was concealed from a primary care physician, diagnoses and prescriptions may be based on incomplete and inaccurate health information. During the study, to show how important it is to access this highly sensitive information, a doctor even told the researcher to follow her to a neighboring doctor's office. When asking about the mental health records, the other doctor replied, *"YES, I want to see that all the time, and I need to know what's going on with my patients!"* In this example, protecting highly sensitive information, on one hand, eliminated bias and improper access, but on the other hand, hindered effective information use among team members. It is worth noting that only at Clinic 1 did we observe the protection of highly sensitive information based on department codes. The other study sites treat all patient information equally.

At Clinic 2, we studied the rollout of an EMR system. As a free outpatient clinic serving the poor, this clinic relies heavily on volunteers to facilitate its daily operations. One main task that was taken on by volunteers prior to EMR adoption was reaching out to patients, either for medical appointments, medication refills, or social services. Prior to the EMR adoption, the clinic had 400 student volunteers who worked on these tasks. Volunteers pulled medical charts from shelves, printed letters, filled in envelopes and called patients using the patient information in their paper records. However, after the system deployment, volunteers lost access to the medical information kept in the EMR and were no longer able to work at the clinic. One reason that accounts for this change is that the EMR treats patient contact information the same as other medical information, and it is no longer accessible to volunteers, since accessing the whole package of the patient's information requires the clinic to purchase user licenses for the constantly changing student volunteers who normally only work in the clinic for a few months. In addition, it is not appropriate for students, who do not have medical expertise, to access private information stored in the records. In the Clinic 2 study, it was clear that treating contact information and other private health information with the same level of sensitivity hindered the information flow in the normal work practices.

The two cases described above indicate that a strict cut-off access for both mental health information and contact information are both inappropriate and blocked the flows of information. These cases raise the question of whether all the private information stored in a patient's medical record should be regarded with the same level of sensitivity, and if there are different levels of sensitivity, that is, whether patient care team members should all be granted the same level of access, regardless of the information needs of their specific role. The earlier descriptions of both dynamic team members and the temporal involvement of team members suggest that core team members who stay with patients and provide long-term medical assistance are in need of accessing the entire spectrum of information. Other peripheral members, such as specialists, technicians, and even volunteers, may only require a small subset of low sensitivity information that is relevant to the completion of their tasks. The cases also suggest that restricting access to a patient's records simply based on the roles a health employee has taken on, instead of whether this person is involved in the patient care process, is not appropriate.

DISCUSSION AND DESIGN IMPLICATIONS

Using cases drawn from our ethnographic studies, we have identified three forms of group dynamics that are unique to health practices, including (a) the constantly changing team members, (b) the dynamic life spans of teams, and (c) the varied sensitivity levels of patient information. These findings fall into four core components outlined in the theory of contextual integrity, as we identified actors (team members), attributes (types of sensitivity), and changes in principles of transmission (time span of the teams). In this section, we discuss how to maintain the right level of appropriateness in medical employees' information practices.

The Appropriate Actors in Context

Nissenbaum's theory [26] suggests that the norms of information flow should be engrained into the daily data practices of medical teams. However, the cases extracted from our field observations show that the boundaries of medical teams are difficult to define in advance, as they are always formed dynamically *in situ* and that the team members of groups are constantly evolving when patient situations change. Because of this, it is not easy to predict the full scope of actors, as it is almost impossible to determine who will be in which patient team before a patient's arrival. For instance, whether a trauma patient in the ED needs an X-ray or MRI exam is dependent on the locations and the type of the injuries a patient has; and whether Dr. Smith or Dr. Taylor will join a patient team may be dependent on their availabilities at that moment.

To address the challenge of dynamic actors, we borrow the token-based access control mechanism proposed in prior study [14] to apply in healthcare context. For example, an ED doctor can grant a token to an EKG technician for a patient's records when s/he orders an EKG test in the EMR system. Or a primary care physician can grant an access token to a physical therapist when a patient is in need of physical therapy treatment. When a link is created to add a team member through an access token, only that member with the access token can view the patient's chart. Under such a mechanism, medical employees who work in the same hospital, but who lack an access token to a patient case, cannot view that patient's chart without first obtaining tokens either through orders or request by an existing team member; the team can dynamically reconfigure as the patient situation changes in context. In doing so, the example of the clinical support members who illegally accessed Giffords' medical records could be prevented before the privacy breach occurred. Meanwhile, if an employee has a valid reason to view highly sensitive

information, s/he can explain the reason for access and obtain a token accordingly.

The Appropriate Information Access

According to Nissenbaum [26], the norms of appropriateness circumscribe how different types of information should be handled or revealed in a given context wherein data practices and actions are performed. Privacy control in medical practices should consider the norms of appropriateness in terms of different types of information, different levels of information sensitivity, and different responsibilities and duties medical employees hold. This suggestion is consistent with the findings of this work that indicate even within a single patient's medical record, there are different levels of information sensitivity. In such cases, adopting an *all-or-nothing* control mechanism can be problematic because such static access-control mechanism does not consider the dynamic norms of information flows in actual medical practices. For instance, in our case of restricting access to mental disease records, the static privacy control mechanism does not incorporate the situations of the legitimate use of these records by family doctors. Likewise, the free clinic study also indicates when the privacy control mismatches with norms of information flows in work practices, it may hinder the work practices supported by patient information. The problems of these one-size-fits-all privacy safeguards reflect the misalignment of privacy management with group-level work practices. That is to say, the norms in actual medical practices were not mapped with the privacy control mechanisms employed by the organizations, where access to patients' records were cut off by departments' codes, or roles' of employees. In other words, access at the right level of appropriateness should be granted to those who need to work on a patient case, regardless of the roles or organizational boundaries of the department.

To address this issue, we suggest role-based access control mechanisms that have been proposed in prior studies [40]. The role-based access control mechanism determines users' access privileges through assigning them with the appropriate roles in the system. Applying this approach to our findings, although group members are dynamic and unpredictable, the cases we described earlier suggest that a patient care team contains both core and peripheral roles, where the core members stay throughout the patient's entire treatment, and the peripheral members only join the team briefly as needed. Since certain roles, such as doctors, are indispensable in a patient care team, information access at the team level can be granted for core members, or the one who first opens a patient chart, and the peripheral members can be added based on their roles. However, this strict access restriction cannot compromise care in an emergency situation. To achieve the balance between information availability and restricted access, a strategy often proposed in this context is "break-the-glass" access [16], in which restrictions can be selectively over-ridden – as if breaking the glass plate that covers a fire alarm – to provide proper access, with the assumption that the threat of a subsequent audit will provide an adequate disincentive for abuse.

The Appropriate Information Transmission

The theory of contextual integrity [27] suggests that, in a given context, transmission principles may change with the changes of other parameters (actors and attributes) and consequently, changes in principles of transmission should be established in context. This notion of establishing changes in transmission principles is extremely important in medical context, since group members are consistently reconfiguring and reforming in context. In temporarily formed medical groups with a high variety of team members, it is obvious that accessing patient information at the time of use should not equal permanent access. On one hand, the information that resides in one's medical records continues to grow and will reach far beyond the amount of information that was granted to a medical employee at the time of access. On the other hand, a one-time access and use of health information does not mean that an employee can always access and use the private information. This temporal dimension is extremely important in dynamic medical teams, since group members are consistently reconfiguring and reforming in context.

The dynamic life span of teams and the volatile time span of different team members make it challenging to define and control the temporal aspect of privacy practices. One strategy that can be proposed to address these challenges is a behavior-based access control mechanism, in which access controls will be built upon an initial set of rules and modified over time based on users' behavioral patterns [20]. Under such an access control mechanism, behavioral logs of the access and use of patients' medical charts and other personal information are analyzed and mined for consistent patterns. For example, mining real behavioral patterns would suggest ED doctors continue accessing a patient's record hours after the patient's discharge for the purpose of documenting progress notes. In such cases, access to patient information can be extended for ED doctors based on the analysis of their behavioral patterns. An effective behavior-based access control mechanism should be able to detect patterns of deviation and provide administrators with feedback and an opportunity to either accept common workarounds; initiate training sessions or interventions to change behavior; or redesign the access control mechanism. More importantly, an effective behavior-based access control mechanism will learn from patterns of behavior, leading to iterative improvements in access management, thereby tightening access options in EMR systems to the minimum necessary rule.

Design Implications

Although our findings highlight the importance of group level privacy practices in the healthcare context, the question of *how* this understanding of group dynamics can be turned into concrete system-level and policy-level recommendations is still a challenge. Clearly illustrated in our study is that a one-size-fits-all privacy policy cannot

accommodate the group dynamics in medical practices. We suggest that it is crucial to align the privacy technologies and policies with users' dynamic needs for data access in context. Towards this end, future research should consider the approach of *Privacy by ReDesign* [9]. This approach indicates that it is not always possible to design appropriate privacy safeguards from the outset; instead, privacy-enhanced solutions should be based on an understanding of the actual system-in-use in real work practices. This notion of redesign is in line with well-recognized design principles in which design of socio-technical solutions is grounded in understanding user behaviors in *context*. Our discussions on group dynamics, in regards to the three layers of contextual integrity, suggest that privacy solutions should consider: (a) establishing appropriate actors in context (defining contextual boundary of dynamic groups), (b) establishing appropriate information access (defining levels of information sensitivity in matching with employees' roles and responsibilities), and (c) establishing changes in principles of transmission (defining pertinent time spans).

In addition, we argue that, because the healthcare information environment is dynamic and event-driven, there are continuous cycles in which procedures need to be updated and re-aligned with new privacy issues or problems that may emerge from work practices. Privacy by redesign should be a continuous and iterative process where constant efforts are expected in ensuring the contextual integrity of privacy in real work practices.

LIMITATIONS AND CONCLUSION

There are several limitations of the study. First, the purpose of this study was not to achieve statistical validation or generalizability but rather to discover patterns for the purpose of better understanding of the main issues in its context. Thus it is reasonable to assume that the findings may not apply to other settings which are distinctly different than what we have studied. Second, the findings are based on the health organizations in U.S., and privacy researchers demonstrated that different countries have approached privacy issues differently in their social norms and regulatory structures [37]. Therefore, a future research opportunity could be to conduct a comparative study in another country.

Though prior research has examined individual-level privacy practices in terms of *how* users react and *what* their privacy practices (via behavioral and technological means) could be, few studies have explored *why* users have reacted the way they do. In this work, we took an approach of studying "*contextually-grounded research that explores privacy issues in the wild* [9]" and addressed the issues of workspace privacy in dynamic medical practices. In particular, we identified group-level dynamics that can be mapped to the contextual integrity theory [26] and argued that group-level privacy is deeply grounded in actual medical practice. Design for group-level privacy compliance is complicated by the fact that team collaborations in health practices are dialectic and dynamic, varying significantly based on the diverse team members, the information appropriateness, and the volatile life span of teams. The insights obtained from our studies on EMR systems point to a new design direction that calls for research focusing on group-level privacy practices. Future designs of privacy control mechanisms should enhance the group-level privacy control features that allow only appropriate team members to access patients' private information while balancing convenient data access with the monitoring and detection of illegitimate access in a real-time fashion.

REFERENCES

1. Agrawal, R. and Johnson, C. Securing Electronic Health Records without Impeding the Flow of Information. *International Journal of Medical Informatics* 76, 5-6 (2007), 471–479.
2. Aronsky, D., Jones, I., Lanaghan, K., and Slovis, C.M. Supporting Patient Care in the Emergency Department with a Computerized Whiteboard System. *Journal of the American Medical Informatics Association* 15, 2 (2007), 184–194.
3. Bardram, J.E. and Bossen, C. Mobility Work: The Spatial Dimension of Collaboration at a Hospital. *Computer Supported Cooperative Work (CSCW)* 14, 2 (2005), 131–160.
4. Barkhuus, L. The mismeasurement of privacy: using contextual integrity to reconsider privacy in HCI. *Proceedings of the CHI 2012*, 367–376.
5. Bauer, L., Cranor, L.F., Reeder, R.W., Reiter, M.K., and Vaniea, K. Real life challenges in access-control management. *Proceedings of CHI 2009*, 899–908.
6. Bélanger, F. and Crossler, R.E. Privacy in the digital age: a review of information privacy research in information systems. *MIS Quarterly*. 35, 4 (2011), 1017–1042.
7. Berg, M. Accumulating and Coordinating: Occasions for Information Technologies in Medical Work. *Computer Supported Cooperative Work (CSCW)* 8, 4 (1999), 373–401.
8. Bulgurcu, B., Cavusoglu, H., and Benbasat, I. Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly* 34, 3 (2010), 523–548.
9. Cavoukian, A. and Prosch, M. Privacy by ReDesign: Building a Better Legacy. 2011. http://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=1070.
10. Chen, Y. Documenting transitional information in EMR. *Proceedings of CHI 2010*, 1787–1796.
11. 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.

12. 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.
13. 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.
14. Dmitrienko, A., Sadeghi, A.-R., Tamrakar, S., and Wachsmann, C. SmartTokens: Delegable Access Control with NFC-enabled Smartphones. *Proceedings of the 5th International Conference on Trust & Trustworthy Computing (TRUST)*, Springer, 325–339.
15. Earp, J.B. and Payton, F.C. Information privacy in the service sector: An exploratory study of health care and banking professionals. *J. Organ. Comp. Electron. Commer.* 16, 2 (2006), 105–122.
16. Ferreira, A., Cruz-Correia, R., Antunes, L., et al. How to break access control in a controlled manner. *Proceedings of the IEEE International Symposium on Computer-Based Medical Systems*, (2006), 847–854.
17. Fitzpatrick, G. and Ellingsen, G. A Review of 25 Years of CSCW Research in Healthcare: Contributions, Challenges and Future Agendas. *Computer Supported Cooperative Work*. (2012). 1-57.
18. Glaser, B.G. and Strauss, A.L. *The discovery of grounded theory*: Strategies for qualitative research. Aldine de Gruyter, Hawthorne, NY, 1967.
19. Grudin, J. Why CSCW applications fail: problems in the design and evaluationof organizational interfaces. *Proceedings of CSCW 1988*, 85–93.
20. Gunter, C.A., Liebovitz, D.M., and Malin, B. Experience-Based Access Management: A Life-Cycle Framework for Identity and Access Management Systems. *IEEE Security and Privacy* 9, 5 (2011), 48–55.
21. Heckle, R., Lutters, W.G., and Gurzick, D. Network authentication using single sign-on: the challenge of aligning mental models. *Proceedings of the Symposium on Computer Human Interaction for Management of Information Technology* (2008), 6:1–10.
22. Kluge, E.H.W. Secure e-Health: Managing Risks to Patient Health Data. *International Journal of Medical Informatics* 76, 5-6 (2007), 402–406.
23. Lee, S., Tang, C., Park, S.Y., and Chen, Y. Loosely formed patient care teams: communication challenges and technology design. *Proceedings of CSCW 2012*, 867–876.
24. Luff, P. and Heath, C. Mobility in collaboration. *Proceedings of CSCW 1998*, 305–314.
25. Murphy, A., Xu, H., Reddy, M., and Ringel, B. Exploring Collaborative Privacy Practices. *CHI 2011 Workshop on Privacy for a Networked World: Bridging Theory and Design.*
26. Nissenbaum, H. Privacy as Contextual Integrity. *Washington Law Review* 79, 1 (2004). 101-139.
27. Nissenbaum, H. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford Law Books, 2009.
28. Ohno-Machado, L., Silveira, P.S.P., and Vinterbo, S. Protecting Patient Privacy by Quantifiable Control of Disclosures in Disseminated Databases. *International Journal of Medical Informatics* 73, 7-8 (2004), 599–606.
29. Palen, L. and Dourish, P. Unpacking "privacy" for a networked world. *Proceedings of CHI 2003*, 129–136.
30. Parks, R., Chu, C.-H., Xu, H., and Adams, L. Understanding the Drivers and Outcomes of Healthcare Organizational Privacy Responses. *Proceedings of 32nd Annual International Conference on Information Systems (ICIS)*, (2011).
31. Parks, R., Chu, C.-H., and Xu, H. Healthcare Information Privacy Research: Issues, Gaps and What Next. *Proceedings of the 17th Americas Conference on Information Systems (AMCIS)*, (2011).
32. Patel, V.L., Arocha, J.F., and Shortliffe, E.H. Cognitive Models in Training Health Professionals to Protect Patients' Confidential Information. *International Journal of Medical Informatics* 60, 2 (2000), 143–150.
33. Peleg, M., Beimel, D., Dori, D., and Denekamp, Y. Situation-Based Access Control: Privacy Management via Modeling of Patient Data Access Scenarios. *Journal of Biomedical Informatics* 41, 6 (2008), 1028–1040.
34. PRC. http://www.privacyrights.org/data-breach. 2012.
35. Reddy, M. and Dourish, P. A finger on the pulse: temporal rhythms and information seeking in medical work. *Proceedings of CSCW 2002.* 344-353.
36. Siponen, M. and Vance, A. Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly* 34, 3 (2010), 487–502.
37. Smith, H.J., Dinev, T., and Xu, H. Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly* 35, 4 (2011), 989–1015.
38. Steinbrook, R. Health Care and the American Recovery and Reinvestment Act. *New England Journal of Medicine* 360, 11 (2009), 1057–1060.
39. Strauss, A., Fagerhaugh, S., Suczek, B., and Wiener, C. *Social Organization of Medical Work*. University of Chicago, Chicago, 1985.
40. Zhang, W., Gunter, C., Liebovitz, D., Tian, J., and Malin, B. Role Prediction using Electronic Medical Record System Audits. *Proceedings of the 2011 American Medical Informatics Association Annual Symposium* (2011), 858–867.
41. Hospital personnel fired for accessing records of Tucson victims. CNN. http://articles.cnn.com/2011-01-12/us/arizona.hospital.records_1_patient-hospital-personnel-medical-records?_s=PM:US.