



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



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

^a College of Information Sciences and Technology, The Pennsylvania State University, USA

^b Department of Communication Studies, Northwestern University, USA

ARTICLE INFO

Article history:

Received 12 January 2015

Received in revised form

11 September 2015

Accepted 25 September 2015

Keywords:

IT Staff

Workarounds

Collaboration

Privacy

Electronic health record (EHR)

Users

ABSTRACT

Purpose: We examined the role of privacy in collaborative clinical work and how it is understood by hospital IT staff. The purpose of our study was to identify the gaps between hospital IT staff members' perceptions of how electronic health record (EHR) users' protect the privacy of patient information and how users actually protect patients' private information in their daily collaborative activities. Since the IT staff play an important role in implementing and maintaining the EHR, any gaps that exist between the IT staff's perceptions of user work practices and the users' actual work practices can result in a number of problems in the configuration, implementation, or customization of the EHR, which can lead to collaboration challenges, interrupted workflow, and privacy breaches.

Methods: We used qualitative data collection methods for this study. We conducted semi-structured interviews with 20 hospital IT staff members. We also conducted observations of EHR users in the in-patient units of the same hospital.

Results: We identified gaps in IT staff's understandings of users' work activities, especially in regards to privacy-compromising workarounds that are used by users and why they are used.

Discussion: We discuss the reasons why this gap may exist between IT staff and users and ways to improve IT staff's understanding of why users perform certain privacy-compromising workarounds.

Conclusion: A hospital's IT staff face a daunting task in ensuring users' collaborative work practices are supported by the system while providing effective privacy mechanisms. In order to achieve both goals, the IT staff must have a clear understanding of their users' practices. However, as this study highlights, there may be a mismatch between the IT staff's understandings of how users protect patient privacy and how users actually protect privacy.

© 2015 Published by Elsevier Ireland Ltd.

1. Introduction

Privacy and collaboration are two central concepts in healthcare. Patient-care teams must continuously share confidential information about patients in order to do their work. However, there are often tradeoffs between sharing patient information to deliver quality and timely healthcare and protecting the patient's information. Health information technologies (HIT), such as the electronic health record (EHR), are meant to facilitate medical employees' collaborative work practices while maintaining mandated levels of patient privacy protection. Protecting patient privacy includes

ensuring the confidentiality, integrity, and security of patient data, as well as ensuring the appropriate use and distribution of patient data [1]. Many EHR systems are designed in a one-size-fits-all fashion by vendors, whose primary privacy focus is on developing security features that meet regulatory and legal requirements. Consequently, information technology (IT) staff in hospitals are faced with the challenge of configuring and customizing these generalized EHR systems so that they adequately support the workflows of hospital staff while still providing effective privacy protection mechanisms [2].

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

* Corresponding author at: Department of Communication Studies, School of Communication, Northwestern University, Evanston, IL 60208, USA.

E-mail address: mreddy@northwestern.edu (M.C. Reddy).

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

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

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

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

sions about subsequent use and distribution of patient data that could result in privacy problems. Therefore, we argue that the task of protecting patient privacy includes not only ensuring the confidentiality, integrity and security of patient data, but also ensuring the appropriate use and distribution of patient information.

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

2. Background

2.1. Collaborative work practices in healthcare

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

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

Download English Version:

<https://daneshyari.com/en/article/516795>

Download Persian Version:

<https://daneshyari.com/article/516795>

[Daneshyari.com](https://daneshyari.com)