AIS Transactions on Human-Computer Interaction

Volume 7 | Issue 3 Article 4

2015

Exploring the Role of Contextual Integrity in Electronic Medical Record (EMR) System Workaround Decisions: An Information Security and Privacy Perspective

A. J. Burns
The University of Texas at Tyler, aburns@uttyler.edu

Jacob Young
Bradley University, jayoung@bradley.edu

Tom L. Roberts
The University of Texas at Tyler, tomroberts@uttyler.edu

James F. Courtney
Louisiana Tech University, courtney@latech.edu

T. Selwyn Ellis
Louisiana Tech University, ellis@latech.edu

Recommended Citation
Burns, A., Young, J., Roberts, T. L., Courtney, J. F., & Ellis, T. S. (2015). Exploring the Role of Contextual Integrity in Electronic Medical Record (EMR) System Workaround Decisions: An Information Security and Privacy Perspective. *AIS Transactions on Human-Computer Interaction, 7*(3), 142-165. Retrieved from https://aisel.aisnet.org/thci/vol7/iss3/4
DOI:

Transactions on Human – Computer Interaction

Research Paper ISSN: 1944-3900

Exploring the Role of Contextual Integrity in Electronic Medical Record (EMR) System Workaround Decisions: An Information Security and Privacy Perspective

Special Issue: HCI in Health and Wellness

A. J. Burns
College of Business and Technology
The University of Texas at Tyler
aburns@uttyler.edu

Jacob Young
Foster College of Business
Bradley University
jayoung@bradley.edu

Tom L. Roberts
College of Business and Technology
The University of Texas at Tyler
Troberts2@uttyler.edu

James F. Courtney
College of Business
Louisiana Tech University
courtney@latech.edu

T. Selwyn Ellis
College of Business
Louisiana Tech University
ellis@latech.edu

Abstract:

Many healthcare providers in the US are seeking increased efficiency and effectiveness by rapidly adopting information technology (IT) solutions such as electronic medical record (EMR) systems. Legislation such as the Health Information Technology for Economic and Clinical Health Act (HITECH), which codified the adoption and "meaningful use" of electronic records in the US, has further spurred the industry-wide adoption of EMR. However, despite what are often large investments in EMR, studies indicate that the healthcare industry maintains a culture of system workarounds. Though perhaps not uncommon, the creation of informal workflows among healthcare workers is problematic for assuring information security and patient privacy, particularly when involving decisions of information management (e.g., information storage, retrieval, and/or transmission). Drawing on the framework of contextual integrity, we assert that one can often explain workarounds involving information transmissions in terms of trade-offs informed by context-specific informational norms. We surveyed healthcare workers and analyzed their willingness to engage in a series of EMR workaround scenarios. Our results indicate that contextual integrity provides a useful framework for understanding information transmission and workaround decisions in the health sector. Armed with these findings, managers and system designers should be better able to anticipate healthcare workers' information transmission principles (e.g., privacy norms) and workaround patterns (e.g., usage norms). We present our findings and discuss their significance for research and practice.

Keywords: Contextual Integrity, Workarounds, Health Information Technology, Privacy, Information Security, Electronic Medical Records (EMR).

1 Introduction

> *[T]echnology [must be] quickly, easily, and safely modified to keep abreast of local conditions; the lack of this capacity results in increasing divergence between "work as imagined" and "work as performed," increasing the articulation work clinicians must perform to bridge this gap, and ultimately leading to a plethora of informal workarounds, all locally reasonable but potentially working at cross-purposes globally.*
>
> —Robert Wears (2015, p. 143)

Due to the essential nature of healthcare, much investment has been made in technology to radically improve the success rate of even the most precarious medical procedures. When compared to other industries, however, concerns over privacy, costs, and reliability have hindered the adoption of information technology (IT) in the health sector over the past several decades (Angst & Agarwal, 2009; Chen & Xu, 2013; Goldschmidt, 2005; Payton, Pare, Le Rouge, & Reddy, 2011; Wu, Wang, & Lin, 2007). In recent years, the promise of IT in healthcare (i.e., health IT[1]) has taken center stage in the US with congressional stimulus for the adoption and "meaningful use" of health IT (e.g., The Health Information Technology for Economic and Clinical Health Act (HITECH)) (Blumenthal, 2010). These stimuli appear to be having the intended effect with health IT adoption rates in the US up dramatically since 2010 (Adler-Milstein et al., 2014).

As in prior studies (e.g., Reardon & Davidson, 2007), in this study, we investigate one type of health IT: electronic medical records (EMR). An EMR system provides a digital record of patients' health-related information that can be "created, gathered, managed, and consulted by authorized clinicians and staff within one health care organization" (Bell, 2008, p. 16). Despite EMR's potential to improve healthcare delivery, merely adopting an EMR system is hardly a panacea for medical efficiency (Blumenthal & Tavenner, 2010). Research indicates that, following their adopting new EMR systems, medical providers often struggle to work in new and evolving systems while maintaining a consistent level of care in a context where service delays and system failures can lead to bodily harm or even death (Goldschmidt, 2005; Spear & Schmidhofer, 2005). Therefore, a successful EMR implementation requires very careful consideration of complex socio-technical issues inherent in the health sector—from conceptualization to implementation (Harrison, Koppel, & Bar-Lev, 2007). For example, a recent working group sponsored by the American Medical Informatics Association (AMIA) recommended that health IT implementations such as EMR systems be designed to comply with legal regulations, provide interoperability, and be flexible enough for both large hospitals and private-practice clinics—all while improving workflow, reducing costs, improving the quality of care, and "maintaining long-standing beneficial patterns of communication" (Kaplan & Harris-Salamone, 2009, p. 292).

System features or functionalities that are perceived to fall short of these established criteria in a given context may lead healthcare providers to resort to "first order problem solving"[2], in which they engage in workarounds to sustain care (Ash, Berg, & Coiera, 2004; Debono et al., 2013; Ferneley & Sobreperez, 2006; Halbesleben & Rathert, 2008; Tucker, 2012). Workarounds are adaptations or improvisations of prescribed processes or procedures to:

> *… overcome, bypass, or minimize the impact of obstacles, exceptions, anomalies, mishaps, established practices, management expectations, or structural constraints that are perceived as preventing that work system or its participants from achieving a desired level of efficiency, effectiveness, or other organizational or personal goals* (Alter, 2014, p. 1044).

Drawing on previous definitions of human-computer interaction (HCI) (e.g., Zhang et al., 2002), we contend that workarounds in the healthcare context emerge as a result of the interaction of information, technologies, and tasks.

[1] The Health Resources and Services Administration defines health IT as the "application of information processing involving both computer hardware and software that deals with the storage, retrieval, sharing, and use of health care information, data, and knowledge for communication and decision making" (HRSA, n.d.).

[2] First-order problem solving (FOPS) comprises problem solving at the point of the conflict such as working around an unresponsive or cumbersome system. This as opposed to second-order problem solving (SOPS), which involves working within the system while seeking change through the appropriate channels (Tucker, 2012).

Although healthcare providers often employ workouts to improve their ability to provide patient care (Debono et al., 2013), when involving the custody of patients' personal health information (PHI) (i.e., any information containing details regarding the health, medical history, or medical treatment of an individual that is personally identifiable (Anderson, 1996)), these workaround decisions may constitute a circumvention of the privacy safeguards built into systems and formalized routines (Murphy, Reddy, & Xu, 2014). Therefore, researchers need to uncover both the system and contextual attributes that influence healthcare workers' decisions to engage in workarounds. Drawing on the framework of contextual integrity, we maintain that, when engaging in workarounds that involve the transmission of PHI, context-specific informational norms play an important role in healthcare workers' decision making process. Contextual integrity is a standard that is "preserved when informational norms are respected and violated when they are contravened" (Nissenbaum, 2009, p. 14).

To examine contextual integrity's role in EMR workarounds, we surveyed healthcare workers and ascertained their willingness to engage in a series of workarounds to EMR systems drawn from previous literature and the popular press. Our findings support contextual integrity as a useful framework for understanding healthcare workers workaround decisions. We present our results and suggest opportunities to incorporate the principles of contextual integrity with system design efforts to reduce workarounds.

2 Background

A key motivation for the recent interest in health IT implementations such as EMR stems from the reality that, in the health sector, information often exists in silos that impede access and lack interoperability (Goldschmidt, 2005). Yet, healthcare is a context in which favorable outcomes require parties to successfully communicate private information with each other. It is this collaborative nature of healthcare that results in disclosure predicaments throughout the course of care provision (Brann & Mattson, 2004; Petronio & Sargent, 2011). To address these shortcomings, stakeholders have looked to EMR systems to increase the efficiency and effectiveness of a notoriously inefficient industry. However, these systems also present new challenges to protect information security and privacy of patients' PHI (Payton et al., 2011).

A complicating issue is the reality that the widespread digitization of health information resulting from increased EMR implementation has also been accompanied by a rise in the number of information security breaches (e.g., unintended disclosure or unsanctioned exposure of PHI). For example, the Ponemon Institute's (2014) Fourth Annual Benchmark Study on Patient Privacy & Data Security found that 90 percent of healthcare organizations have had at least one data breach in the 2010-2013 period, and 38 percent reported that they had more than five incidents in 2013. This statistic is up from only 29 percent that reported more than five incidents from 2008 to 2010. Further, the Identity Theft Resource Center (ITRC) recently reported that the healthcare industry is one of the most affected industries, accounting for 43.8% of the all known breaches and exposing over 8.8 million records (ITRC, 2014).

These breach statistics highlight an important dichotomy: the digitization of health information has the potential to increase both legitimate and illegitimate use of sensitive health information. The novel risks to information security and privacy that EMR systems pose mandate the implementation of security protocols to maintain the confidentiality of PHI, yet these new responsibilities create workflow disruptions (Unertl, Novak, Johnson, & Lorenzi, 2010) and often result in resistance from healthcare professionals to implement privacy measures (Bulgurcu, Cavusoglu, & Benbasat, 2010). The Office of the National Coordinator for Health Information Technology (ONC) lists workflow adoption as a "top 5" issue for implementing security and privacy measures (DHS, 2013). The implication is that, when faced with an overly rigid/inefficient way of interacting with EMR, healthcare providers often choose to work around inconveniences, or perceived inefficiencies, to attend to the pressing needs of the situational context (Ash et al., 2004; Debono et al., 2013; Koppel, Wetterneck, Telles, & Karsh, 2008; Tucker, 2012). In this way, context is a primary driver of workaround rationalization. For example, Debono et al. (2013, p. 11) describes tensions among nurses' rationalizations:

> *… [o]n the one hand, studies reported workaround behaviors as necessary to deliver care or in the best interest of the patient. However, nurses also identified them as unsafe in particular contexts and as workarounds are not legally sanctioned, some nurses perceived them as professionally risky.*

Based on these reflections, we can see that healthcare professionals' perception of a workaround's appropriateness varies according to its nature.

2.1 Workarounds

Regardless of the system type, healthcare professionals need to consider two important factors when evaluating workarounds: motivation and consequence. For example, Ferneley and Sobreperez (2006) identify three classifications of workarounds: (1) hindrance workarounds, (2) harmless workarounds, and (3) essential workarounds. Table 1 summarizes these general classifiers of workarounds.

Table 1. General Classifiers Workarounds

Classification	Description of workarounds[i]	Implication
Hindrance	Hindrance workarounds are aimed at circumventing a "system procedure or process perceived to be too time consuming, onerous, or difficult" (p. 347).	Not necessarily malicious, but short-term gain in users' workflow is accompanied by an overall diminution of system performance—particularly as it relates to ancillary goals such as security and privacy.
Harmless	Harmless workarounds are those user-generated routines that are not supported by the current system but, at the same time, do not inhibit its intended function.	Reflect workflow preferences or system capabilities not supported by the system and may provide a roadmap for future system enhancements.
Essential	Essential workarounds are those user-prescribed procedures that are deemed essential to the overarching goal of the users' job role.	Reflect an essential capability that is lacking in the current system and are likely to be viewed in a workgroup as an acceptable practice. Often become incorporated into the behavioral norms among employees[ii].

[i] From Ferneley & Sobreperez (2006); [ii] Button, Mason, & Sharrock (2003), Kobayashi, Fussell, Xiao, & Seagull (2005)

Relating specifically to our context of interest, Friedman et al. (2014) describe workarounds observed in the healthcare environment on the following three dimensions: (1) whether the workaround was temporary or routinized (i.e., long term, ongoing), (2) whether the workaround was avoidable or unavoidable, and (3) whether the workaround was deliberately chosen or unplanned. Table 2 summarizes these descriptors of workarounds.

Table 2. Descriptors of Workarounds (Friendman et al., 2014, p. e81-e82)

Temporary/routinized	Temporary workarounds are "short-term solutions to a time delimited problem", whereas a routinized workarounds "become part of the regular workflow"
Avoidable/unavoidable	Avoidable workarounds are procedures that solve an issue that could otherwise have been avoided permanently (e.g., through appropriate system design and/or use), whereas unavoidable workarounds occur when some uncontrollable external constraint impacts a system user's work processes.
Deliberate/unplanned	Deliberate workarounds imply an "explicit, self-reflexive decision" in order to address a particular system limitation, whereas unplanned workarounds arise unforeseen along the course of care.

The classifiers in Table 1 and the descriptors in Table 2 complement each other in describing workarounds in the health sector. Therefore, one can classify a single workaround as one of the following: hindrance, harmless, or essential, and further describe them as temporary or routinized, avoidable or unavoidable, and deliberate or unplanned. For example, one might classify a healthcare worker's reverting to paper documents when the electronic system is unavailable in an emergency situation as essential and described as temporary, unavoidable, and unplanned. However, these classifications and descriptors are dependent on the context surrounding the behavior and the attributes of the EMR system. That is, the same workaround may be avoidable in one scenario and unavoidable in another scenario based on the current EMR system and context. These classifications and descriptors are manifest in the context of the workaround decisions and influence the perception that engagement in a given workaround will preserve or violate contextual integrity.

2.2 Contextual Integrity

Contextual determinants often define the appropriate flow of information, a principle termed contextual integrity (Nissenbaum, 2009). Contextual integrity is a multi-dimensional framework that characterizes norms (and norm violations) in terms of (1) contexts, (2) actors, (3) attributes, and (4) transmission principles (Chen & Xu, 2013; Nissenbaum, 2009). In the IS literature, contexts are known to be an important factor in determining an individual's privacy preferences (e.g., Bélanger & Crossler, 2011; Conger, Pratt, & Loch, 2013; Mason, 1986). Specifically, contexts are "structured social settings characterized by canonical activities, roles, relationships, power structures, norms (or rules), and internal values (goals, ends, purposes)" (Nissenbaum, 2009, p. 132). According to its definition, context is a multi-dimensional concept. Roles define the capacities in which individuals act in certain contexts, and relationships characterize the interactions and dependencies arising therein. Related to roles and relationships, norms define the "duties, obligations, prerogatives, and privileges associated with particular roles, as well as acceptable and unacceptable behaviors" (Nissenbaum, 2009, p. 133). Lastly, values reveal the teleology of the context and define the ultimate purpose of the context and individuals' shared principles. The context-relative informational norms are summarized in Table 3.

Table 3. Context-relative Informational Norms (Nissenbaum, 2009)

Contexts	Backdrop of informational norms (i.e., healthcare)
Actors	Senders of information, recipients of information, and information subjects
Attributes	Information types, nature of information, data fields
Transmission principles	Constraint on the flow (distribution, dissemination, transmission) of information from party to party in a context. The transmission principle parameter in informational norms expresses terms and conditions under which such transfers ought (or ought not) to occur (p.145).

2.3 Contextual Integrity as a Decision Framework

Contextual integrity provides a robust framework for violations of privacy wherein a violation of contextual integrity signals a prima facie violation of privacy (Nissenbaum, 2009). As such, the framework can also be used as a decision framework to determine whether or not an action constitutes a violation of privacy in a given context. By assessing the context relative norms, one can establish the appropriate data flow for the context. Therefore, establishing the contextual characteristics of a transmission informs the transmission principles.

To test for violations of contextual integrity, one must first establish the transmission's contexts, actors, and attributes. Based on these characteristics, the transmission principles are established. A red flag is the extent to which a new practice or proposed action is seen as a violation of the informational norms (i.e., violates contextual integrity) (Nissenbaum, 2009). Table 4 summarizes these foundations of contextual integrity.

Table 4. Foundations of Contextual Integrity (Nissenbaum, 2009)

Contexts	Establish prevailing context
Actors	Establish key actors
Attributes	Ascertain what attributes are affected
Transmission principles	Establish changes in principles of transmission Determinants: confidentiality, deservedness, entitlement, compulsion, need
Red flag	If the new practice generates changes in actors, attributes, or transmission principles, the practice is flagged as violating entrenched informational norms and constitutes a prima facie violation of contextual integrity (p.150).

2.4 Healthcare as Context

As we note previously, context refers to activities, roles, relationships, norms, and values (Nissenbaum, 2009). Therefore, to establish the healthcare context, we must distinguish these distinct yet related contextual factors. In healthcare, as with many contexts, roles often determine the nature of activities, relationships, norms, and even values (Nissenbaum, 2009). There are essentially three roles that are of

importance in the healthcare context: (1) medical experts and medical support staff (i.e., doctors/nurses), (2) operations support staff (other healthcare professionals such as technicians and administrators), and (3) patients (Paul, Ezz, & Kuljis, 2012). For this study, we focus on those who provide healthcare (e.g., the first two groups) and the distinctions between them because medical experts and their operations support staff are the primary users of EMR systems. To ascertain the contextual differentiation between those that directly dispense care (i.e., doctors/nurses) and operational support (i.e., other healthcare providers), we seek guidance from the most admired work in Western medical ethics, the Hippocratic Oath (Miles, 2005).

Hippocrates' original oath pledged to respect confidentiality: ''What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself, holding such things shameful to be spoken about'' ("Oath of Hippocrates", 1995, p. 2632). Based in millennia of practice, the right to health information privacy is universally recognized and has been codified in many countries with laws such as the Health Insurance Portability and Accountability Act (HIPAA) in the US (Appari & Johnson, 2010). The primary impetus for this law was the protection of PHI from potential threats to patient confidentiality emanating from electronic healthcare transactions (Moskop, Marco, Larkin, Geiderman, & Derse, 2005).

Though first administered some 2,500 years ago, modern versions of the Hippocratic Oath continue to be taken by many physicians and it largely governs the ideal teleology of the healthcare industry (Antoniou et al., 2010; Tyson, 2001). Today, one can summarize the oath in three principles: (1) beneficence, (2) non-maleficence, and (3) confidentiality (Kirch, 2008). These three guiding principles largely inform the activities, relationships, norms, and values of doctors/nurses, while operations support staff are more guided by legalism (i.e., operating in the legal framework).

Implicit in the first two principles is the notion that doctors/nurses first and foremost are concerned with preserving life (i.e., (1) whenever possible, heal; and (2) never harm). These principles form the basis for the informational norms for doctors/nurses in the healthcare context. We contend that confidentiality, rather than being merely a guiding principle, is a procedural directive mandated by HIPAA and HITECH. That is, concerns over protecting private information are secondary only to the pursuit of the primary goal: to care for patient's health (Timmons, 2003). The primary teleology of healthcare further informs decisions regarding the trade-off often required between privacy and performance (Tentori, Favela, & González, 2006; Xu, Luo, Carroll, & Rosson, 2011).

Contextual integrity stipulates that the actors themselves contribute to contextual norms. We contend that actors' personal characteristics, such as age and gender, are an important consideration, particularly in the healthcare context. For example, a recent survey of U.S. physicians indicates an age gap in EMR adoption. According to the report from the U.S. Center of Disease Control (CDC), 64 percent of physicians under the age of 50 use EMR, while only approximately half of physicians above 50 have adopted electronic records (Jamoom et al., 2012). Previous research has also established gender differences among physician communication and patient centricity. For example, in a meta-analysis, female primary care providers were found to spend more time with patients and have greater patient-centered communication (Roter, Hall, & Aoki, 2002).

3 Study

Based on our discussion of the contextual nature of privacy perceptions and the prevalence of systems workarounds in healthcare, we examine healthcare professionals' decisions to engage in EMR system workarounds. Specifically, we employ the contextual integrity framework to assess the role of informational norms in healthcare workers' decisions to work around EMR systems.

3.1 Establishing the Context of Study

To explore the role of contextual integrity in workaround decisions, we first established a context for the decisions. As we note previously, central to the concept of contextual integrity are the transmission principles that determine factors such as entitlement, deservedness, compulsion, and need for the workaround decision. To establish the context of decisions, we developed scenarios based on responses from healthcare professionals regarding their use of EMR published in previous research (Ilie, Courtney, & Van Slyke, 2007; Ilie, Van Slyke, Parikh, & Courtney, 2009) and the popular press (e.g., Carollo, 2011; Gray & Herbert, 2007; Hutchinson, 2011). By drawing the scenarios from prior healthcare research and reports of actual incidences, we followed the tactics of prior researchers (e.g., Nagin & Pogarsky, 2001; Piquero & Hickman, 1999; Siponen & Vance, 2010) to increase the realism and relevance of our

scenarios for our respondents. Additionally, we introduced each scenario with a quote from a fellow healthcare provider explaining the system's short-comings that the workaround circumvents from the user's perspective.

The vignettes describe behaviors in the healthcare context as defined by the roles, relationships, norms, and values. The roles represented in our vignettes are specific to healthcare providers, and the relationship depicted is the relationship between healthcare provider and patient. The norms are defined by the obligations arising between patient and healthcare provider. Finally, sustaining life and providing care comprise the healthcare industry's over-arching teleology. Table 5 summarizes the context of the vignettes from the perspective of contextual integrity.

Table 5. Context-relative Informational Norms

Contexts		Healthcare workarounds
Actors	**Senders**	Healthcare professionals
	Recipients	Self/other healthcare professionals
	Subjects	Patient
Attributes		Health records (PHI)

3.2 Pilot Study

We originally considered six workarounds as potential scenarios in the early stages of this research. Ultimately, we selected four scenarios for the full study after considering the qualitative responses provided by a pilot study conducted with a group of healthcare professionals. We adapted three of the four vignettes employed in this study from prior research, which included quotes from physician residents and attending physicians employed at an outpatient clinic collected over a two year period in a large hospital facility in the southern United States after it had implemented an EMR system (Ilie et al., 2007; Ilie, Van Slyke, Courtney, & Parikh, 2008; Ilie et al., 2009). We developed the remaining vignette (scenario 4) from published media accounts of healthcare responses following natural disasters, such as those experienced following Hurricane Katrina and the 2011 tornado which severely damaged St. John's Regional Medical Center in Joplin, Missouri (e.g., Carollo, 2011; Gray & Herbert, 2007; Hutchinson, 2011). We provided participants of both the pilot and full study with a quote from a physician regarding the EMR system and a brief description of steps that the healthcare providers took to work around the issue. Table 6 includes the classification and descriptions of each scenario along with a summary of the perceived HCI issues leading to the workaround. We report the full vignettes in Appendix 2. In Section 3.3, we summarize the vignette and behavioral decision depicted in the scenarios.

3.3 Scenarios

Scenario 1: *A healthcare provider uses a file transfer app on a personal device to transfer unencrypted patient records from a hospital computer to a personal computer to review patient treatment plans at home.*

The first scenario involved a deliberately chosen hindrance workaround due to the willful disregard of acceptable security practices for external access to the EMR system in response to the perceived inconvenience of security token use. In prior research (e.g., Ilie et al., 2007; Ilie et al., 2008), investigators found that physicians often felt that using a security token to authenticate their identity was unreliable and unnecessarily burdensome because it delayed or prevented access to patient information. Drawing from these experiences, scenario 1 described a workaround of a trusted system that used security token authentication. It explained a hindrance workaround enabled by the use of a file transfer app on a personal device to remove unencrypted files from the healthcare facility for offsite review. The vignette concluded with the information that the physician would update patient files in the secure system prior to beginning their next shift.

Scenario 2: *A group of healthcare providers each remain logged into the EMR system at separate terminals so that all providers have access to the system from each terminal.*

The second scenario described a routinized hindrance workaround in response to a perceived shortcoming in an EMR system. The scenario described a system that required users to log in and out

several times throughout the course of patient care, resulting in workflow disruption (e.g., Ilie et al., 2007; Ilie et al., 2008). When a physician failed to log out of a terminal anywhere in the hospital, the physician would be prevented from accessing the EMR system until they had retraced their steps—sometimes across multiple floors—and successfully logged out of the previous terminal. According to the vignette, to minimize this interruption, healthcare providers conspired to share credentials by leaving all terminals logged in simultaneously. While this workaround clearly addressed the need for patient data access, it exposed the organization to significant risk at the expense of patient privacy. Therefore, this scenario exhibited a workaround that can arise due to poor EMR system design and implementation and the failure to respond to user feedback.

Scenario 3: *Instead of logging into the healthcare facility's electronic medical records (EMR) system to retrieve and enter patient information, a healthcare provider delegates the responsibilities to a nurse to spend more time treating patients.*

Scenario three described a routinized harmless workaround in which a physician relied on support staff, such as nurses and assistants, to retrieve patient data in an effort to spend more time treating patients rather than using the EMR system (e.g., Ilie et al., 2007; Ilie et al., 2008). Although the perceived inefficiencies of the EMR system use led physicians to delegate their system use to other employees, we can consider such behavior to be an acceptable practice in terms of patient privacy.

Scenario 4: *A healthcare provider used a personal smartphone to quickly arrange the transfer of patients in critical condition to another facility. The provider also used the same personal smartphone to email screenshots of patient files to the receiving facility.*

The final scenario exhibited a temporary essential workaround and involved a physician's actions following a natural disaster. The authors developed this particular scenario was developed following a review of news articles published in the aftermath of various crises which affected healthcare facilities (Carollo, 2011; Gray & Herbert, 2007; Hutchinson, 2011). In this vignette, we depicted a scenario in which a tornado had rendered a medical facility's auxiliary power source unusable, which prevented healthcare providers from accessing the EMR system. According to the vignette, the facility had no formalized routine for health information transmissions in the case of catastrophic power failure. In response, the healthcare provider depicted in this scenario resorted to using their own personal device to communicate with and transfer patient files to those facilities accepting patient transfers from the damaged facility.

Table 6. Study Vignette Classifications and Descriptions

Scenario	Perceived HCI issue	Workaround summary	Classification	Descriptors
Scenario 1	Overly burdensome and unreliable file transfer process	Personal file transfer app	Hindrance	Temporary, avoidable, deliberate
Scenario 2	Login routine causes workflow disruption	Remaining logged in	Hindrance	Routinized, avoidable, deliberate
Scenario 3	Interaction with EMR system takes time away from patients	Delegation	Harmless	Routinized, avoidable, deliberate
Scenario 4	Lack of a formalized emergency back-up for catastrophic power failure	Personal smartphone after tornado	Essential	Temporary, avoidable, unplanned

3.4 Hypotheses

Based on the contextual integrity framework, we generated our hypotheses about healthcare providers' willingness to engage in EMR system workarounds. As we noted in Table 5, the context of the transmission depends on the workaround scenario, the actors are healthcare professionals, and the attributes are PHI. Therefore, to shed light on contextual integrity's role in explaining workaround decisions involving PHI, we examine differences among actors and across transmission contexts.

3.4.1 Context: Workaround Scenario

A primary tenet of the contextual integrity framework is that red flag behaviors are considered violations of privacy. We contend that, in healthcare, individual scenarios create context for which norms define the acceptability of behavior. In other words, we can summarize the context of each scenario in terms of its classification and descriptors. Therefore, we hypothesize the degree to which the behavior depicted in each scenario is perceived by the healthcare providers to be a violation of contextual integrity (red flag) will be negatively related to a healthcare worker's willingness to engage in the workaround (main effect).

H1: *The degree to which a behavior violates contextual integrity (raises a red flag) is negatively related to a healthcare worker's likelihood of engaging in the behavior (scenario → engagement).*

3.4.2 Actors: Role

In addition to the context the scenario provides, the contextual integrity of a transmission behavior is also dependent on each actor's role. In the healthcare context, the role of the healthcare worker determines the informational norms. Due to the over-arching teleology of healthcare idealized in the Hippocratic Oath, we contend that, in healthcare, doctors and nurses are more sensitive to violations of contextual integrity arising from the transmission principles of an individual scenario. Therefore, we hypothesize an interaction between scenario and job role (doctors/nurses and other healthcare professionals).

H2: Doctors/nurses and other healthcare professionals vary in their willingness to engage in the workarounds across scenarios (scenario X role → engagement)

3.4.3 Actors: Individual Characteristics

Previous research has established the importance of individual characteristics in affecting decisions related to IT use with moral or ethical dimensions (Leonard et al., 2004). As we mention previously, researchers have found age and gender to be individual characteristics that influence behavior in this domain (Leonard, Cronan, & Kreie, 2004; Roter et al., 2002). We hypothesize gender differences in work around decisions by scenario. Further, based on gender differences found in the healthcare sector (e.g., female physicians), we hypothesize a three-way interaction between scenario, role, and gender.

H3: *Healthcare professionals' willingness to engage in the workarounds varies by gender across scenarios (scenario X gender → engagement).*

H4: *Doctors/nurses' and other healthcare professionals' willingness to engage in the workarounds varies by gender and role across scenarios (scenario X role X gender → engagement).*

3.5 Controls

3.5.1 Age

As we mention previously, age is also an individual characteristic that has IT-use implications. In the healthcare sector, a recent survey of U.S. physicians revealed that physicians over 50 are less likely to adopt EMR (Jamoom et al., 2012). We include age as a control in our study.

Central to the context of transmission decisions in healthcare is the organizational context. We controlled for several important organizationally related factors.

3.5.2 Security Training Frequency

First, we included the frequency of security training as a measure of the healthcare worker's security education, training, and awareness (SETA). We also contend that including SETA frequency should control for the organization's security focus.

3.5.3 Sector

Another potentially significant contextual factor in healthcare is the sector in which the healthcare worker provides care. We included the context of the health sector as a control in our study (i.e., public, private, not-for-profit).

3.5.4 Organizational Tenure

Contextual integrity is founded on the influence of informational norms in transmission decisions. To control for the influence that organizational tenure may have in influencing the importance of such norms, we included organizational tenure as a control in our study.

3.6 Sample

To test our hypotheses, we surveyed healthcare professionals working in the United States using an online panel. Our final sample size was 177. Table 7 summarizes the cross-sectional panel of healthcare professionals' statistics. Panels are an accepted source of survey data, especially when the topic (such as EMR system workarounds) requires full anonymity and not simply confidentiality. Providing anonymous, off-site access to self-report surveys has been shown to be adequate and appropriate for eliciting self-reported incidences of security-related behaviors (e.g., protection-motivated behaviors (Posey, Roberts, Lowry, Bennett, & Courtney, 2013)) and even socially undesirable behaviors such as organizational deviance (Bennett & Robinson, 2000, 2003).

Table 7. Descriptive Statistics of Sample

Average age		49.9
Average organizational tenure (years)		12.3
Sex	Female	54.2%
	Male	45.8%
Job role	Doctor/nurse	41.8%
	Other health professionals	58.2%
Sector	Public	32.8%
	Private	35.0%
	Not-for-profit	32.2%
EMR		75.1%

3.7 Instrumentation

We took a within-subjects approach (repeated measures) and provided vignettes to our sample of healthcare professionals that described scenarios of system workarounds taken by a healthcare provider. We chose vignettes for our study because they are especially apt at eliciting contextual norms (Finch, 1987). We developed our study following the precedent and recommendations of prior scenario-based research (e.g. D'Arcy, Hovav, & Galletta, 2009; Siponen & Vance, 2010, 2014). Because we exposed our respondents to multiple scenarios that were unrelated to one another, we controlled for the possibility of an ordering bias by randomizing the order of the vignettes for each respondent, an effective counterbalancing technique (Warner, 2008). As we note previously, we piloted a version of our instrument with a group of healthcare professionals before executing the full survey.

3.7.1 Likelihood of Engagement

Immediately following each scenario, we asked our respondents to indicate the likelihood that they would engage in the same behavior exhibited in each scenario. As in other studies, we used the single item measurement to capture our respondents' willingness to enact a behavior (Leonard et al., 2004; Siponen & Vance, 2010). The use of single item measures immediately following a scenario is widely accepted in the IS literature and meets the "most appropriate" threshold espoused by methodologists for single-item measures (Siponen & Vance, 2010; Straub, Boudreau, & Gefen, 2004).

3.7.2 Red Flag

In the contextual integrity framework, transmissions that violate entrenched norms are said to raise a "red flag". To assess the degree to which the behaviors described in each scenario violate entrenched norms (raise a "red flag"), we included two items measuring contractualism from prior research (Reidenbach & Robin, 1990). Violations of contractualism are behaviors that violate a context's implied obligations, contracts, duties, and rules (Reidenbach & Robin, 1990). We contend that the degree to which a behavior

violates the implied obligations, duties, or rules of a context should correspond to the degree to which the behavior raises a "red flag". The items ask respondents the degree to which the behavior violates (1) an unwritten contract and (2) an unspoken promise (Reidenbach & Robin, 1990).

4 Analyses

To examine the role of contextual integrity in healthcare providers' workaround decisions, we first assessed the degree to which the behavior of each scenario raised a red flag among our respondents; we then followed-up with a multiple analysis of variance (MANOVA) to assess our hypotheses.

4.1 Red Flag Ratings

Contextual integrity provides a privacy decision making heuristic, and contexts stipulate obligations arising from roles, relationships, norms, and values. To assess the red flag raised by each scenario, we asked respondents to rate the behavior on two contractualism items. The two items exhibited strong reliability for each scenario, and two scenarios rated relatively low on the contractualism scale, while two rated relatively high. In the terms of contextual integrity, we refer to these as relatively small and large red flags raised by the behavior. Table 8 includes the construct statistics of the contractualism items and the overall red-flag ratings of each scenario.

Table 8. Scenario Red Flag Ratings

Scenario	Red flag	Mean	Std. deviation	Cronbach's α
Scenario 1	Large	5.26	1.78	0.977
Scenario 2	Large	5.09	1.84	0.978
Scenario 3	Small	3.40	1.84	0.969
Scenario 4	Small	3.51	1.75	0.951

These red flag ratings further support the presence of context-relative informational norms in healthcare. Scenarios 1 and 2 were large violations of contextual integrity (and, thus, had higher red-flag ratings) because they exhibited a tradeoff of patient privacy for healthcare providers' convenience (e.g., "hindrances"). Conversely, scenarios 3 and 4 both exhibited workarounds that enhanced providers' ability to serve the overriding goal of the healthcare context (and thus had relatively lower red-flag ratings when compared to scenarios 1 and 2). For example, scenario 3 depicted a workaround that exhibits a tradeoff between system use and time spent with patients (e.g., "harmless"), and scenario 4 depicted an essential workaround caused by a catastrophic system failure (e.g., "essential"). Figure 1 exhibits the healthcare providers' red-flag assessment of each scenario.

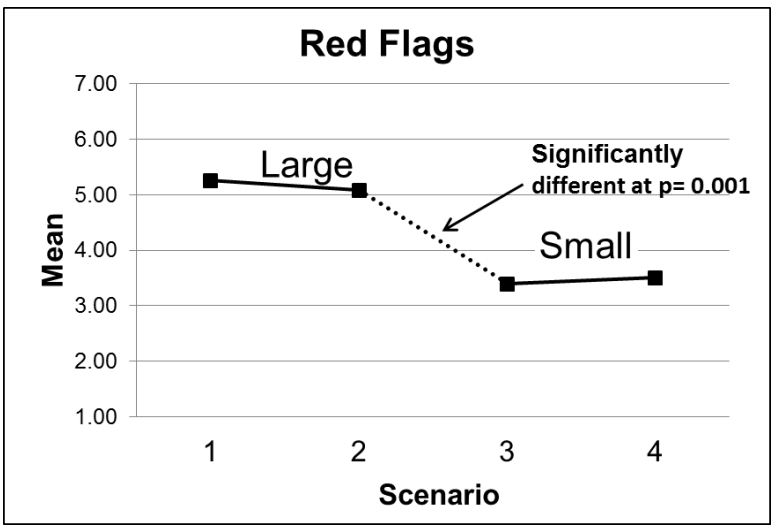

Figure 1. Scenario Red Flag Ratings

4.2 Results

We examined our hypotheses with a MANOVA on the four dependent variables (likelihood of engagement) to test for unequal engagement in workarounds across the scenarios. We included the main effect of the scenario (1), the interaction effects of job role and scenario (H2) and gender and scenario (H3), and the three-way interaction between job role, gender, and scenario (H4). Our scenarios constituted a four-level within-subject factor. Table 8 summarizes the corresponding subsample sizes for our categorical variables.

Table 9. Breakdown of Sample

	Males	Females	Totals
Doctors/nurses	n = 31	n = 43	n = 74
Other Healthcare professionals	n = 50	n = 53	n = 103
Totals	n = 81	n = 96	n = 177

4.3 MANOVA

We chose MANOVA because of its suitability for: (1) research designs with less than or equal to four levels, and (2) our large number of participants (i.e., greater than number of treatments + 15) (Algina & Keselman, 1997; Warner, 2008). Additionally, MANOVA is a robust procedure (Warner, 2008). We also assessed of statistical power (Cohen, 1988). Table 10 summarizes the results of the MANOVA.

Table 10. MANOVA Results

Hypothesis	Wilks' lambda	F-value	P-value	Observed power [i]
H1: scenarios → engagement	0.941	3.320	0.021*	0.75
H2: scenarios * role → engagement	0.973	1.469	0.225	0.38
H3: scenarios * gender → engagement	0.964	1.973	0.120	0.50
H4: scenarios * gender * role → engagement	0.938	3.527	0.016*	0.78
Controls				
Age * scenario→ engagement	0.994	0.328	0.805	0.11
SETA * scenario → engagement	0.954	2.575	0.056	0.63
Sector * scenario → engagement	0.941	1.657	0.131	0.63
Tenure * scenario → engagement	0.979	1.130	0.339	0.30
Box's test of equality of covariance matrices: Box's M = 129.218 (p= 0.460); absolute values of skewness & kurtosis for DVs < |1|; [i]alpha = 0.05 * p < 0.05; bold = supported.				

The first hypothesis (H1) concerns the influence of the scenario's context on the decision to work around an EMR system. Our results indicate that the decision to work around an EMR system varies by transmission scenario. We further hypothesized that decisions to work around EMR systems correspond with the extent to which the workaround violates contextual integrity (raises a red flag). Table 11 summarizes the descriptive statistics of the likelihood of engagement item for each scenario. Appendix A shows the means and standard deviations of our sample (separated by gender and role).

Table 11. Engagement—Descriptive Statistics

Scenario	Mean	S.D.	N
Scenario 1—engagement	2.57	1.85	177
Scenario 2—engagement	2.81	2.06	177
Scenario 3—engagement	4.44	1.99	177
Scenario 4—engagement	4.98	1.90	177

Figure 2 exhibits the willingness to engage in the workaround for each scenario given the red flag raised by the behavior.

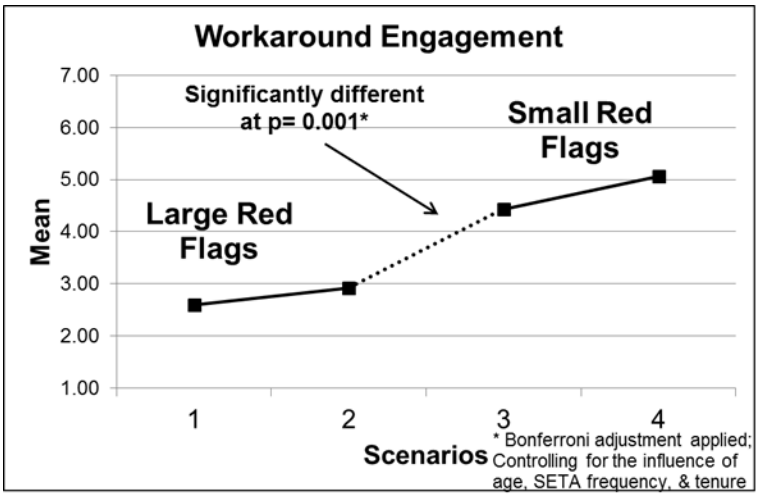

Figure 2. Workaround Engagement by Scenario

As Table 10 shows, however, H2 and H3 were not supported. We found no significant interaction found between scenario and role (scenario X role) or between scenario and gender (scenario X gender). However, we did find support for H3: a three-way interaction between scenario, gender, and role (scenario X gender X role). Figures 3 and 4 plot the three-way interaction.

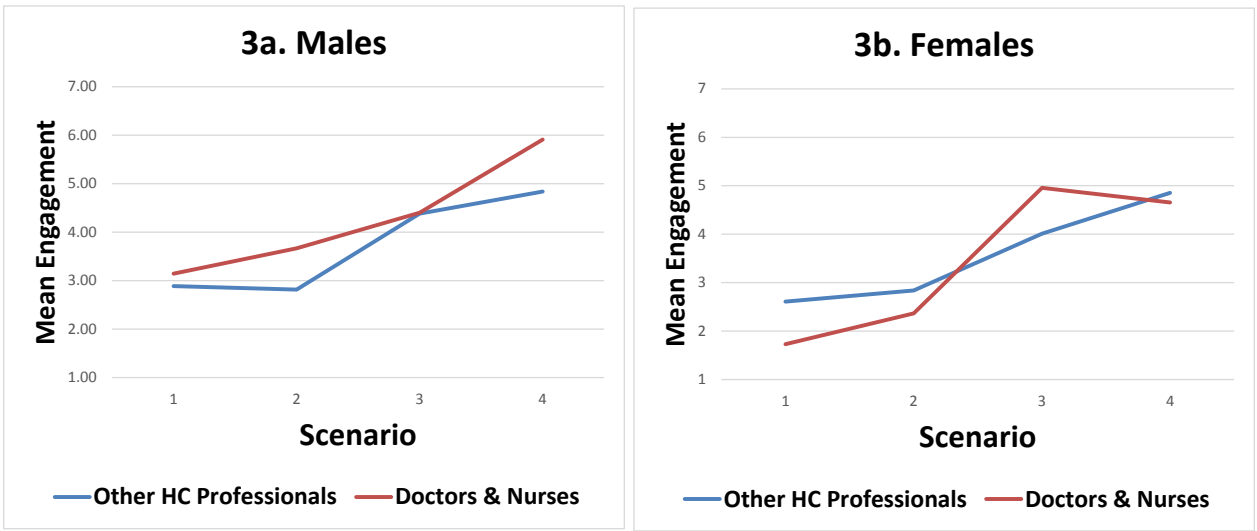

Figure 3. Three-way Interactions: Males & Females Plotted Separately

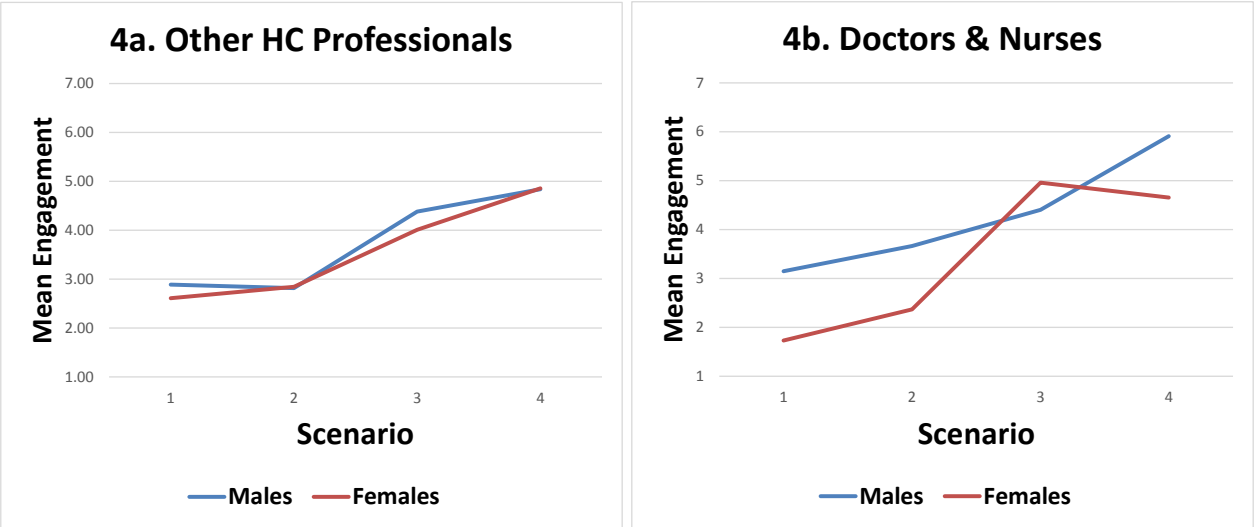

Figure 4. Three-way Interactions: Healthcare Roles Plotted Separately

5 Discussion

In this study, we examine the role of context in healthcare professionals' workaround decisions related to EMR systems. Drawing on the concept of contextual integrity, we assessed the influence of contextual determinants in healthcare professionals' willingness to engage in system workarounds. We first established the red flags raised by each of four vignettes that we provided to our respondents by ascertaining the degree to which a behavior violates an implied obligation (i.e., contractualism). We then employed a mixed-model research design to ascertain within-subject effects attributable to principles of contextual integrity. We found support for the contextual nature of within-subject healthcare decisions with scenario significantly impacting willingness to engage. Further, the base hypothesis from contextual integrity was supported with significant differences between the vignettes depicting large red flag behaviors and the vignettes depicting small red flag behaviors. Interestingly, we found that the two workarounds classified as hindrances (per Table 6) were both associated with large red flags by our panel of healthcare professionals.

Further, we found support for a three-way interaction between job role, gender, and scenario. Figures 3a and 3b plot the engagement of doctors/nurses and other healthcare professionals separately for males and females. First, for all males, doctors/nurses consistently exhibited a greater willingness to work around systems across scenarios than others (per Figure 3a), while female doctors/nurses were less likely to work around existing systems than others in all but one scenario (i.e., scenario 3 (see Figure 3b)). Female doctors/nurses exhibited the least willingness to engage in the hindrance workarounds across all groups (i.e., all males and non-doctor/nurse females), which perhaps reveals an increased sensitivity to violations of contextual integrity. Further, in support of our hypotheses and in concert with previous findings, females were the most likely to engage in harmless delegation when it provided increased time spent with patients (i.e., scenario 3). In fact, this was the only scenario for which female doctors/nurses' willingness was the highest of all groups.

Comparing Figures 3a and 3b also sheds light on important differences between genders across job roles. As we can see, males had the greatest agreement across job roles on the willingness to work around in scenarios 1 (file transfer app) and 3 (delegation), while females exhibited the greatest agreement across job roles on the willingness to work around the EMR system in scenarios 2 (remaining logged in) and 4 (smartphone after tornado).

Figures 4a and 4b show the three-way interaction with doctors/nurses and other healthcare providers plotted separately. The consistency of non-doctors/nurses' willingness to engage in workarounds in each scenario across genders is quite conspicuous (Figure 4a). However, Figure 4b exhibits the interaction effect with clear gender differences among doctors/nurses. Across genders, doctors/nurses exhibited pronounced differences between behaviors raising a similar red flag, which evidences their increased sensitivity to scenario-specific privacy concerns over that of other healthcare providers. For example,

among doctors/nurses, males were more willing to engage in system workarounds in all but scenario 3 (i.e., delegation). Interestingly, when the workaround was deemed essential (scenario 4), male doctors/nurses were most likely to engage in a workaround above all other groups.

6 Implications and Contributions

Our findings offer insights for practitioners and researchers interested in HCI in the healthcare context, where our application of contextual integrity to workarounds is an important example of the interaction among information, technologies, and tasks. Further, we believe healthcare is a particularly promising setting for contextual integrity because it is a hyper-connected, information-rich environment with longstanding informational norms and communication patterns that inform information transmission decisions. Healthcare is also one of the few industries where privacy has been codified by law (i.e., HIPAA) in the United States. In addition, healthcare decision making often has life-or-death consequences that can override privacy with more critical duties. Supported by the framework of contextual integrity, we examined healthcare professionals' willingness to engage in EMR system workarounds. By using vignettes, we were also able to drill down into the context of each scenario to ascertain significant contextual determinants of each scenario. In this way, our within-subjects design serves as a novel application of the contextual integrity framework.

As the Hippocratic roots of the health sector implies, our findings seem to confirm that healthcare professionals' workaround decisions are influenced by their prioritizing patient care over preserving privacy. Though healthcare is a highly regulated industry, in the course of caring for patients, the legalistic view is often usurped by informational norms that help explain privacy-related decisions. We found that the behaviors in scenarios 1 and 2 (those that did not directly impact patient care) were more likely to raise a red flag among healthcare professionals and less likely to be engaged in than the behaviors in scenarios 3 and 4. This finding suggests that healthcare professionals across all roles are less inclined to engage in workaround behaviors that do not directly impact patient treatment. It also signals that healthcare professionals are more worried about their primary goal of treating and saving patients' lives than the secondary goal of privacy. These findings have implications for academics, policy makers, and IS designers. Applying the contextual integrity framework augments the ability of stakeholders to anticipate both privacy and usage norms for health-IT. For example, in light of these results, developers can test new transmission principles prescribed in policies, procedures, interfaces, and systems—regardless of their specific features—for violations of contextual integrity (i.e., red flags) to limit workarounds. We contend that understanding transmission principles of the context is an important step in designing systems and artifacts that are both secure and effective.

We also isolated the actors in the healthcare professionals. We found differences between those directly treating the patients (doctors/nurses) and those who were part of the healthcare process but who did not directly treat patients. Importantly, we found that doctors/nurses were more sensitive to the context of individual transmissions than other healthcare professionals. This increased sensitivity was amplified when we plotted males and females separately across job roles (i.e., Figures 4a and 4b). These results occurred even though HIPAA and privacy laws have been in place for nearly two decades, which illustrates the role of contextual integrity as determinants of IT usage and privacy norms in healthcare. The significant interaction between job role, gender, and scenario highlights the complexity of privacy-considerations in the healthcare domain.

Our findings also affirm the idea that privacy laws are not absolute and can be overridden by more critical considerations and duties (Moskop et al., 2005). Researchers should find this result informative because it helps to isolate the impact of context on privacy in an environment that is extremely regulated. It also opens up questions about context in unregulated environments where the norms range widely. For practice, these results present the reality of conflicting goals and transmission dilemmas in healthcare.

Finally, this research adds to the substantial work investigating IT adoption in the medical field. While many studies have examined the adoption of health IT and EMR, relatively few have examined use and workarounds in the way that we have. For example, rather than studying firm-level adoption of EMR, we investigate health-related workarounds that occur at the individual level. Additionally, our work highlights the importance of designing systems that minimize the trade-off between privacy and performance in healthcare.

6.1 Limitations and Opportunities for Future Research

While we believe our findings are instructive for research and practice, we note some inherent limitations in our approach. First, we relied on self-reported measures to capture healthcare workers' willingness to engage in workarounds. However, to counter this weakness, we provided anonymous, off-site surveys, which is an accepted practice for security and privacy research. As in prior research, we also used vignettes based on actual workarounds to enhance the scenarios' relatability to the respondents.

Second, we examined an important, but limited, set of contextual determinants (i.e., scenario, gender, and role). Future research could build on these findings through experimental manipulation of the system design features to establish the design standards and system capabilities that minimize the tradeoff between working in and working around the prescribed IT environment (e.g., the establish factors that increase the perceived red flag of a workaround behavior). Table 12 relates the determinants of context-specific informational norms to the design lifecycle. Additionally, though we included controls for SETA frequency, we did not capture the content of the SETA programs. Future research should investigate an organization's ability to influence informational norms through specific SETA initiatives.

Table 12. Contextual Integrity and Information System Design

Development phase	Determinants of informational norms
Planning	• **Contexts**: Establish the range of relevant contexts for the planned system • **Actors**: Establish the key actors' perspectives needed to design the system • **Attributes**: Establish the attributes of information required • **Transmission principles**: Establish the principles that ensure the contextual integrity of information transmissions in the system.
Analysis	• **Contexts**: Determine the contexts for which the system is currently designed and isolate coverage gaps • **Actors**: Determine the actors' perspectives currently considered in the design and identify missing perspectives • **Attributes**: Determine the set of attributes for which the system is designed and identify missing attributes • **Transmission principles**: Determine the principles implicit in the current system and compare with those consistent with contextual integrity
Design	• **Contexts**: Design system for appropriate contexts • **Actors**: Design system taking into account the appropriate perspectives and access needs • **Attributes**: Design system to account for specified attributes • **Transmission principles**: Design system to maintain contextual integrity, including the associated IT and interface design
Implementation	• **Contexts**: Implement system within specified contexts • **Actors**: Provide access to appropriate actors with their respective access-levels • **Attributes**: Populate with appropriate attributes • **Transmission principles**: Train users on the informational norms upheld by the system to decrease workarounds
Maintenance	• **Contexts**: Monitor for changes in contexts or the need to account for new contexts • **Actors**: Monitor the perspectives of actors to be considered • Attributes: Assess appropriateness of attributes and monitor for new attributes of importance • **Transmission principles**: Monitor the informational norms emerging from systems' use and configure training and/or system updates taking informational norms into account. Identify workarounds and redesign system if necessary.

Finally, our findings also highlight an emerging issue of employees using personally owned devices for organizational purposes. Two of our scenarios included a healthcare professional using their own device to work around the EMR system. This trend has been dubbed "bring your own device" (BYOD) and is having a profound impact on enterprise as 89 percent of U.S. firms now enable some form of BYOD (Bradley, Loucks, Macaulay, Medcalf, & Buckalew, 2012). Whether personally owned or issued by the organization, mobile devices such as the ones depicted in our vignettes are becoming commonplace in healthcare environments with well over 50 percent of doctors using laptops, smartphones, and/or tablets for medical purposes (McGee, 2012). Privacy risks are exacerbated with mobile devices due to their

portability, and 78 percent of technology professionals have cited lost or stolen devices as a major concern with mobile computing (Finneran, 2013). Even prominent hospitals, such as the Beth Israel Deaconess Medical Center (a Harvard University teaching hospital) in Boston, have grappled with privacy issues related to a stolen personal laptop containing unencrypted patient information (Cerrato, 2012). Future research should further examine the role of BYOD and mobile technology in workaround and compliance decisions.

7 Conclusion

In closing, we believe that healthcare is a unique context in which to examine privacy-related behaviors. As legislation continues to prod the healthcare industry toward wholesale conversion to EMR, the ability to understand workaround decisions is paramount to the success of these legislative initiatives. We amplify our contributions by incorporating the workaround culture that exists within healthcare. We largely agree with Nissenbaum (2009) that the duty of healthcare professionals to regulate the flow of information in context of care is fiduciary. As such, contextual integrity is well suited to the healthcare context, which implies an obligation to act in the patient's best interest rather than to maintain confidentiality or protocol. Until systems and artifacts are developed in anticipation of usage and privacy norms in healthcare (e.g., as informed through the framework of contextual integrity), we contend that workarounds at the individual level will likely continue to plague this vital industry regardless of legislative initiative and institutional IT investments.

Acknowledgments

The first author performed part of this work as a Postdoctoral Research Scholar in the Owen Graduate School of Management at Vanderbilt University and acknowledges support from the National Science Foundation (NSF) project on Trustworthy Health and Wellness—CNS-1329686. The views and conclusions expressed are those of the authors and should not be interpreted as representing the views, either expressed or implied, of NSF.

References

Adler-Milstein, J., DesRoches, C. M., Furukawa, M. F., Worzala, C., Charles, D., Kralovec, P., Stalley, S., & Jha, A. K. (2014). More than half of US hospitals have at least a basic EHR, but stage 2 criteria remain challenging for most. *Health Affairs*, *33*(9), 1664-1671.

Algina, J., & Keselman, H. (1997). Detecting repeated measures effects with univariate and multivariate statistics. *Psychological Methods*, *2*(2), 208-218.

Alter, S. (2014). Theory of workarounds. *Communications of the Association for Information Systems*, *34*, 1041-1066.

Anderson, R. J. (1996). A security policy model for clinical information systems. In *Proceedings of the IEEE Symposium on Security and Privacy* (pp. 30-43).

Angst, C. M., & Agarwal, R. (2009). Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. *MIS Quarterly*, *33*(2), 339-370.

Antoniou, S. A., Antoniou, G. A., Granderath, F. A., Mavroforou, A., Giannoukas, A. D., & Antoniou, A. I. (2010). Reflections of the Hippocratic Oath in modern medicine. *World Journal of Surgery*, *34*(12), 3075-3079.

Appari, A., & Johnson, M. E. (2010). Information security and privacy in healthcare: Current state of research. *International Journal of Internet and Enterprise Management*, *6*(4), 279-314.

Ash, J. S., Berg, M., & Coiera, E. (2004). 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), 104-112.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly*, *35*(4), 1017-1042.

Bell, K. (2008). Report to the office of the national coordinator for health information technology on defining key health information technology terms. *The National Alliance for Health Information Technology*. Retrieved from https://www.nachc.com/client/Key%20HIT%20Terms%20Definitions%20Final_April_2008.pdf

Bennett, R. J., & Robinson, S. L. (2000). Development of a measure of workplace deviance. *Journal of Applied Psychology*, *85*(3), 349-360.

Bennett, R. J., & Robinson, S. L. (2003). The past, present, and future of workplace deviance research. In J. Greenberg (Ed.), *Organizational behavior: The state of the science* (2nd ed., pp. 247-281). Mahwah, NJ: Lawrence Erlbaum Associates.

Blumenthal, D. (2010). Launching HIteCH. *New England Journal of Medicine*, *362*(5), 382-385.

Blumenthal, D., & Tavenner, M. (2010). The “meaningful use” regulation for electronic health records. *New England Journal of Medicine*, *363*(6), 501-504.

Bradley, J., Loucks, J., Macaulay, J., Medcalf, R., & Buckalew, L. (2012). BYOD: A global perspective. *Cisco Internet Business Solutions Group*. Retrieved from http://resources.idgenterprise.com/original/AST-0074924_BYOD_Horizons-Global.pdf

Brann, M., & Mattson, M. (2004). Toward a typology of confidentiality breaches in health care communication: An ethic of care analysis of provider practices and patient perceptions. Health Communication, 16(2), 231-251.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. MIS Quarterly, 34(4), 523-548.

Button, G., Mason, D., & Sharrock, W. (2003). Disempowerment and resistance in the print industry? Reactions to surveillance–capable technology. *New Technology, Work and Employment*, *18*(1), 50-61.

Carollo, K. (2011). Joplin, Missouri: Hospital deemed unsafe after tornado, all patients evacuated. *ABCNews.com*. Retrieved from http://abcnews.go.com/Health/joplin-mo- hospital-evacuated-sustaining-extensive-tornado-damage/story?id=13666314

Cerrato, P. (2012). Halamka knows perils and promise of healthcare BYOD. *Information Week*. Retrieved from http://www.informationweek.com/mobile/halamka-knows- perils-and-promise-of-healthcare-byod/d/d-id/1107822

Chen, Y., & Xu, H. (2013). Privacy management in dynamic groups: understanding information privacy in medical practices. In *Proceedings of the 2013 Conference on Computer Supported Cooperative Work* (pp. 541-552).

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2nd ed.). Hillsdale, NJ: Lawrence Erlbaum Associates.

Conger, S., Pratt, J. H., & Loch, K. D. (2013). Personal information privacy and emerging technologies. *Information Systems Journal*, *23*(5), 401-417.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, *20*(1), 79-98.

Debono, D. S., Greenfield, D., Travaglia, J. F., Long, J. C., Black, D., Johnson, J., & Braithwaite, J. (2013). Nurses' workarounds in acute healthcare settings: A scoping review. *BMC Health Services Research*, *13*(1), 175.

DHS. (2013). Update on the adoption of health information technology and related efforts to facilitate the electronic use and exchange of health information. *United States Department of Human Services*. Retrieved from http://www.healthit.gov/sites/default/files/rtc_adoption_of_healthit_and_relatedeffor ts.pdf

Ferneley, E. H., & Sobreperez, P. (2006). Resist, comply or workaround? An examination of different facets of user engagement with information systems. *European Journal of Information Systems*, *15*(4), 345-356.

Finch, J. (1987). The vignette technique in survey research. *Sociology*, *21*(1), 105-114.

Finneran, M. (2013). 2013 state of mobile security. *Information Week*. Retrieved from http://reports.informationweek.com/abstract/18/10935/Mobility-Wireless/Research:-2013-State-Of-Mobile-Security.html

Friedman, A., Crosson, J. C., Howard, J., Clark, E. C., Pellerano, M., Karsh, B.-T., Crabtree, B., Jaén, C. R., & Cohen, D. J. (2014). A typology of electronic health record workarounds in small-to-medium size primary care practices. *Journal of the American Medical Informatics Association*, *21*(e1), e78-e83.

Goldschmidt, P. G. (2005). HIT and MIS: Implications of health information technology and medical information systems. *Communications of the ACM*, *48*(10), 68-74.

Gray, B. H., & Herbert, K. (2007). Hospitals in Hurricane Katrina: Challenges facing custodial institutions in a disaster. *Journal of Health Care for the Poor and Underserved*, *18*(2), 283-298.

Halbesleben, J. R., & Rathert, C. (2008). The role of continuous quality improvement and psychological safety in predicting work-arounds. *Health Care Management Review*, *33*(2), 134-144.

Harrison, M. I., Koppel, R., & Bar-Lev, S. (2007). Unintended consequences of information technologies in health care—an interactive sociotechnical analysis. *Journal of the American Medical Informatics Association*, *14*(5), 542-549.

HRSA. (n.d.). What is health IT? *Health Resources and Services Administration*. Retrieved from http://www.hrsa.gov/healthit/toolbox/oralhealthittoolbox/introduction/whatishealthit.html

Hutchinson, C. (2011). Joplin, MO: Was tornado-hit hospital properly prepared? *ABCNews.com*. Retrieved from http://abcnews.go.com/Health/WellnessNews/joplin-mo-tornado-hit-hospital-properly-prepared/story?id=13685614

Ilie, V., Courtney, J., & Van Slyke, C. (2007). P*aper versus electronic: Challenges associated with physicians-usage of electronic medical records*. Paper presented at the 40th Annual Hawaii International Conference on Systems Sciences, Waikoloa, Big Island, HI.

Ilie, V., Van Slyke, C., Courtney, J. F., & Parikh, M. A. (2008). *From mouse to pen: Inhibiting effects of security measures on physicians' usage of electronic medical records* (working paper).

Ilie, V., Van Slyke, C., Parikh, M. A., & Courtney, J. F. (2009). Paper versus electronic medical records: The effects of access on physicians' decisions to use complex information technologies. *Decision Sciences*, *40*(2), 213-241.

ITRC. (2014). 2013 data breach stats. *Identity Theft Resource Center*. Retrieved from http://www.idtheftcenter.org/images/breach/UPDATED_ITRC_Breach_Stats_Report_Summary_2013.pdf

Jamoom, E., Beatty, P., Bercovitz, A., Woodwell, D., Palso, K., & Rechtsteiner, E. (2012). Physician adoption of electronic health record systems: United States, 2011. *U.S. Department of Health and Human Services*. Retrieved from http://www.cdc.gov/nchs/data/databriefs/db98.pdf

Kaplan, B., & Harris-Salamone, K. D. (2009). Health IT success and failure: Recommendations from literature and an AMIA workshop. *Journal of the American Medical Informatics Association*, *16*(3), 291-299.

Kirch, W. (Ed.). (2008). *Encyclopedia of public health*. New York, NY: Springer.

Kobayashi, M., Fussell, S. R., Xiao, Y., & Seagull, F. J. (2005). Work coordination, workflow, and workarounds in a medical context. In *Proceedings of the Extended Abstracts on Human Factors in Computing Systems* (pp. 1561-1564).

Koppel, R., Wetterneck, T., Telles, J. L., & Karsh, B.-T. (2008). Workarounds to barcode medication administration systems: Their occurrences, causes, and threats to patient safety. *Journal of the American Medical Informatics Association*, *15*(4), 408-423.

Leonard, L. N., Cronan, T. P., & Kreie, J. (2004). What influences IT ethical behavior intentions—planned behavior, reasoned action, perceived importance, or individual characteristics? *Information & Management*, *42*(1), 143-158.

Mason, R. O. (1986). Four ethical issues of the information age. *MIS Quarterly*, *10*(1), 5-12.

McGee, M. (2012). Healthcare IT 2012 priorities survey: Government mandates dominate. *Information Week*. Retrieved from http://reports.informationweek.com/abstract/105/8692/Healthcare/research-healthcare-it-2012-priorities-survey.html

Miles, S. H. (2005). The Hippocratic oath and the ethics of medicine. Oxford, UK: Oxford University Press.

Moskop, J. C., Marco, C. A., Larkin, G. L., Geiderman, J. M., & Derse, A. R. (2005). From Hippocrates to HIPAA: Privacy and confidentiality in emergency medicine—part I: conceptual, moral, and legal foundations. *Annals of Emergency Medicine*, *45*(1), 53-59.

Murphy, A. R., Reddy, M. C., & Xu, H. (2014). Privacy practices in collaborative environments: A study of emergency department staff. In *Proceedings of the 17th ACM Conference on Computer Supported Cooperative Work & Social Computing* (pp. 269-282).

Nagin, D. S., & Pogarsky, G. (2001). Integrating celerity, impulsivity, and extralegal sanction threats into a model of general deterrence: Theory and evidence. *Criminology*, *39*(4), 865-892.

Nissenbaum, H. (2009). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford, California: Stanford University Press.

Oath of Hippocrates. (1995). In W. Reich (Ed.), *The encyclopedia of bioethics*. New York, NY: MacMillan.

Paul, R. J., Ezz, I., & Kuljis, J. (2012). Healthcare information systems: A patient-user perspective. *Health Systems*, *1*(2), 85-95.

Payton, F. C., Pare, G., Le Rouge, C. M., & Reddy, M. (2011). Health care IT: Process, people, patients and interdisciplinary considerations. *Journal of the Association for Information Systems*, *12*(2), i-xiii.

Petronio, S., & Sargent, J. (2011). Disclosure predicaments arising during the course of patient care: Nurses' privacy management. *Health Communication*, *26*(3), 255-266.

Piquero, A. R., & Hickman, M. (1999). An empirical test of Tittle's control balance theory. *Criminology*, *37*(2), 319-342.

Ponemon Institute. (2014). Fourth annual benchmark study on patient privacy & data security. *Ponemon Institute, LLC*. Retrieved from https://www2.idexpertscorp.com/ponemon-report-on-patient-privacy-data-security-incidents/

Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., & Courtney, J. F. (2013). Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. *MIS Quarterly*, *37*(4), 1189-1210.

Reardon, J. L., & Davidson, E. (2007). An organizational learning perspective on the assimilation of electronic medical records among small physician practices. *European Journal of Information Systems*, *16*(6), 681-694.

Reidenbach, R. E., & Robin, D. P. (1990). Toward the development of a multidimensional scale for improving evaluations of business ethics. *Journal of Business Ethics*, *9*(8), 639-653.

Roter, D. L., Hall, J. A., & Aoki, Y. (2002). Physician gender effects in medical communication. *Journal of the American Medical Association*, *288*(6), 756-764.

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly*, *34*(3), 487-502.

Siponen, M., & Vance, A. (2014). Guidelines for improving the contextual relevance of field surveys: The case of information security policy violations. *European Journal of Information Systems*, *23*(3), 289-305.

Spear, S. J., & Schmidhofer, M. (2005). Ambiguity and workarounds as contributors to medical error. *Annals of Internal Medicine*, *142*(8), 627-630.

Straub, D. W., Boudreau, M. C., & Gefen, D. (2004). Validation guidelines for IS positivist research. *Communications of the Association for Information Systems*, *13*, 380-427.

Tentori, M., Favela, J., & González, V. M. (2006). Quality of privacy (QoP) for the design of ubiquitous healthcare applications. *Journal of Universal Computer Science*, *12*(3), 252-269.

Timmons, S. (2003). A failed panopticon: Surveillance of nursing practice via new technology. *New Technology, Work and Employment*, *18*(2), 143-153.

Tucker, A. (2012). *Work design drivers of organizational learning about operational failures: A laboratory experiment on medication administration* (Working paper no. 13-044). Harvard Business School.

Tyson, P. (2001). The Hippocratic oath today. *NOVA: Public Broadcasting System*. Retrieved from http://www.pbs.org/wgbh/nova/body/hippocratic-oath-today.html

Unertl, K. M., Novak, L. L., Johnson, K. B., & Lorenzi, N. M. (2010). Traversing the many paths of workflow research: Developing a conceptual framework of workflow terminology through a systematic literature review. *Journal of the American Medical Informatics Association*, *17*(3), 265-273.

Warner, R. M. (2008). *Applied statistics: From bivariate through multivariate techniques*. Thousand Oaks, CA: Sage.

Wears, R. L. (2015). Health information technology and victory. *Annals of Emergency Medicine*, *65*(2), 143-145.

Wu, J., Wang, S., & Lin, L. (2007). Mobile computing acceptance factors in the healthcare industry: A structural equation model. *International Journal of Medical Informatics*, *76*(1), 66-77.

Xu, H., Luo, X. R., Carroll, J. M., & Rosson, M. B. (2011). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision Support Systems*, *51*(1), 42-52.

Zhang, P., Benbasat, I., Carey, J., Davis, F., Galletta, D. F., & Strong, D. (2002). AMCIS 2002 panels and workshops I: Human-computer interaction research in the MIS discipline. *Communications of the Association for Information Systems*, *9*, 334-355.

Appendix A

Table A1. Full Descriptive Statistics across All Scenarios

Scenario 1	**Males**	**Females**	**Totals**
Doctor/nurse mean (s.d.)	n = 31 3.26 (2.14)	n = 43 1.77 (1.32)	n = 74 2.39 (1.86)
Other mean (s.d.)	n = 50 2.82 (1.97)	n = 53 2.58 (1.71)	n = 103 2.70 (1.84)
Totals mean (s.d.)	n = 81 2.99 (2.03)	n = 96 2.22 (1.60)	N = 177 2.57 (1.85)
Scenario 2	**Males**	**Females**	**Totals**
Doctor/nurse mean (s.d.)	n = 31 3.65 (2.27)	n = 43 2.35 (1.66)	n = 74 2.89 (2.03)
Other mean (s.d.)	n = 50 2.86 (2.06)	n = 53 2.64 (2.13)	n = 103 2.75 (2.10)
Totals mean (s.d.)	n = 81 3.16 (2.16)	n = 96 2.51 (1.93)	N = 177 2.81 (2.06)
Scenario 3	**Males**	**Females**	**Totals**
Doctor/nurse mean (s.d.)	n = 31 4.65 (1.98)	n = 43 4.95 (1.89)	n = 74 4.82 (1.92)
Other mean (s.d.)	n = 50 4.26 (2.05)	n = 53 4.08 (1.98)	n = 103 4.17 (2.01)
Totals mean (s.d.)	n = 81 4.41 (2.02)	n = 96 4.47 (1.98)	N = 177 4.44 (1.99)
Scenario 4	**Males**	**Females**	**Totals**
Doctor/nurse mean (s.d.)	n = 31 5.84 (1.34)	n = 43 4.65 (2.15)	n = 74 5.15 (1.94)
Other mean (s.d.)	n = 50 4.84 (1.96)	n = 53 4.87 (1.82)	n = 103 4.85 (1.88)
Totals mean (s.d.)	n = 81 5.22 (1.81)	n = 96 4.77 (1.97)	N = 177 4.98 (1.90)

Appendix B: Full Vignettes and Instrumentation

Scenario 1

"My problem with the electronic medical record (EMR) system is that if you're out of the hospital, you have to use this security token that I can't stand because I don't always have the token with me. Plus, sometimes it takes a couple of times to get it to work. You want something that's fast and this is like dial-up versus cable."

After completing each shift, instead of accessing the EMR system remotely using a security token (a device used to prove one's identity electronically), the healthcare provider used a file transfer app on a personal device to transfer unencrypted patient records from a hospital computer to a personal computer in order to review patient treatment plans at home. Prior to starting the next shift, the healthcare provider updates patient records with any necessary changes.

Scenario 2

"The problem with the electronic medical record (EMR) system is that if you log into the system to check on a patient on the 2nd floor and you forget to log off, when you get up to the 10th floor to check on another patient, you're locked out of the system. Sometimes I am locked out and don't remember where I was last logged in and then I'm stuck! I can't log on again; it's a big problem! I have to call everywhere I've been and have someone see if I forgot to log out. Sometimes they will just log me off, but it's a big problem! You have to trace yourself backwards. It's pathetic!"

After two years of regular requests made to the EMR system administrator asking for the implementation of an automated logout feature, a group of healthcare providers eventually decided to each remain logged into the EMR system at separate terminals so that all providers have access to the system from each terminal.

Scenario 3

"I have my nurse with me and she can look the results up in the electronic medical record (EMR) system for me and have them ready when I get to the patient's room because I'm busy. I will go see a patient, then go do a procedure and then come back to see another patient, and another patient, then go upstairs and do something else."

Instead of logging into the healthcare facility's electronic medical records (EMR) system to retrieve and enter patient information, a healthcare provider delegated the responsibilities to a nurse in order to spend more time treating patients.

Scenario 4

"The tornado destroyed our auxiliary power and prevented us from being able to access our electronic medical record (EMR) system. All we had available to us was the latest hard copy of each patient's file. Since the building was not safe, we knew we had to evacuate as soon as possible. We eventually sent all of our critical patients by ambulance to a facility over an hour away."

After a medical facility loses electricity following a tornado and backup generators fail to keep essential equipment functioning, a healthcare provider used a personal smartphone to quickly arrange the transfer of patients in critical condition to another facility. The provider also used the same personal smartphone to email screenshots of patient files to the receiving facility so that they could prepare for the arrival of patients.

Survey Items:

Engagement item: "Please rate the likelihood that you would engage in the same behavior exhibited in the scenario".

(1) I would not engage in this activity—(7) I would engage in this activity

Contractualism items: "Please rate the behavior on the following scale…"

(1) Does not violate an unspoken promise—(7) Does violate an unspoken promise

(1) Does not violate an unwritten contract—(7) Does violate an unspoken contract

About the Authors

A. J. Burns is an Assistant Professor in the College of Business and Technology at The University of Texas at Tyler. He earned his DBA in Computer Information Systems from Louisiana Tech University and his BS and MBA from Louisiana State University. He was previously a Postdoctoral Research Scholar in the Owen Graduate School of Management at Vanderbilt University where he worked on a large multi-institutional, interdisciplinary team studying trustworthy health and wellness. His research interests include emerging issues in security and privacy impacting individuals, organizations, and societies. His work has been published in peer reviewed journals and presented at international conferences.

Jacob Young is currently a Doctoral Candidate in the College of Business at Louisiana Tech University and an Assistant Professor of Management Information Systems at Bradley University. He received his BS and MBA from Henderson State University. His primary research area is the ethics of information systems use, including privacy, security and anonymity. His dissertation focuses on the impact of perceived anonymity on the use of whistle-blowing systems. His work has been presented at several national and regional conferences.

Tom L. Roberts is Department Chair for Computer Science and Professor of Information Systems at the College of Business and Technology at the University of Texas at Tyler. He was formerly the Director of the Center of Information Assurance, Information Systems Coordinator and Clifford R. King Professor of Information Systems at Louisiana Tech University. He previously held academic appointments at the University of Kansas, the University of Central Florida, and Middle Tennessee State University. He received his MBA and PhD in Information Systems from Auburn University and BA degree from the University of Oklahoma. He has published over 40 refereed journal papers and book chapters and has more than 60 conference proceedings and presentations. This list includes publications in many top journals such as *MIS Quarterly, Journal of Management Information Systems, Journal of the Association for Information Systems*, *Information Systems Journal, European Journal of Information Systems*, *Information & Management*, *Computers & Security*, *IEEE Transactions in Software Engineering*, *IEEE Transactions in Engineering Management, IEEE Transactions on Professional Communication*, and others.

James (Jim) F. Courtney is Professor of Computer Information Systems and holder of the Humana Foundation - McCallister Eminent Scholar Chair in the Management & Information Systems Department at Louisiana Tech University. He formerly was Professor of Information Systems at the University of Central Florida and Tenneco Professor of Business Administration in the Information and Operations Management Department at Texas A&M University. His academic experience also includes faculty positions at Georgia Tech, Texas Tech, Lincoln University in New Zealand and the State University of New York at Buffalo. He received his PhD in Business Administration (Management Science) from the University of Texas at Austin in 1974. He has published over 45 refereed papers in several different journals, including *Management Science, MIS Quarterly, Communications of the ACM, IEEE Transactions on Systems, Man and Cybernetics, Decision Sciences, Decision Support Systems*, the *Journal of Management Information Systems*, *Database*, the *Journal of the Association of Information Systems,* and the *Journal of Applied Systems Analysis*. He has also published over 60 papers in refereed conference proceedings and book chapters. His present research interests are knowledge-based decision support systems, healthcare information systems, information assurance, ethical decision making, knowledge management, inquiring (learning) organizations and sustainable economic systems.

T. Selwyn Ellis is the Balsey-Whitmore Endowed Professor in Business at Louisiana Tech University. He earned his Doctor of Business Administration degree from Louisiana Tech University. His research interests include IT ethics and information assurance. He has published papers in various journals such as *European Journal of Information Systems*, the *DATABASE for Advances in Information Systems*, *Journal of Computer Information Systems*, and *the European Journal of Operational Research*.

Transactions on Human – Computer Interaction

Editors-in-Chief

http://thci.aisnet.org/