Healthcare Professionals' Attitudes towards Privacy in Healthcare Information Systems

Submission Type: Full Paper

Michael Lapke
University of Mary Washington
mlapke@umw.edu

Christopher Garcia
University of Mary Washington
cgarcia@umw.edu

David Henderson
University of Mary Washington
dhender3@umw.edu

Abstract

As a result of the Health Information Technology for Economic and Clinical Health Act (HITECH), healthcare organizations are finding themselves scrambling to digitize their Electronic Medical Records (EMRs). A concern of the widespread implementation of digital health records is the assurance of privacy for the sensitive information held by healthcare organizations (Greenberg, 2010; Hoffmann, 2009). There have been many studies that examine patient's perspectives and expectations of privacy (Agarwal & Anderson, 2011; Cannoy & Salam, 2010) but the literature is lacking analysis of healthcare providers' privacy perspectives with regards to EMRs. Using Information Boundary Theory (Stanton, 2002) as a theoretical framework, this study seeks to determine healthcare providers' attitudes towards privacy with regards to EMRs. Analysis of survey data collected from healthcare providers found that healthcare providers do not value patient privacy over personal or organizational gain.

Keywords

Healthcare Information Technology, Healthcare, Privacy, Electronic Medical Records

Introduction and Argument

The Health Information Technology for Economic and Clinical Health Act (HITECH) became law in 2009. This was part of the federal stimulus legislation known as the American Reinvestment and Recovery Act. The legislation aimed to provide more than $20 billion to get doctors and hospitals to use electronic medical records, computerized prescription systems and other health information technology (HIT). The bill dictated that if doctors can't demonstrate "meaningful use" of certified electronic health record system by 2015, they face reduced Medicare payments.

In February 2011, at the Health Information and Management Systems Society annual meeting, Kathleen Sebelius, secretary of Health and Human Services, told care providers "In the last two years, the share of primary care providers using a basic electronic health record has gone from under 20 percent to nearly 30 percent." She also pointed out that "When President Obama came into office, only two in 10 doctors used even a basic electronic health record system. Over the last two years, we've created unprecedented momentum behind health information technology."

As HIT is ramping up both internally and as a result of government legislation, privacy advocates have expressed concern for the vulnerability of individual's health information. In contrast, the public is generally positive in regards to the rapid digitization of medical records. A study in 2010 found that 77%

of patients were amenable to letting hospitals, clinics or physicians store their digital health records (Greenberg, 2010). Another survey in 2011 reported that 81% of patients have a positive perception of documenting patient care electronically.

This positive outlook by health consumers is surprising given the number of highly publicized cases of security breaches at medical facilities in recent years. For example, the recent 2015 data breach at Anthem Health exposed the personal information of about 80 million patients. It is the largest data breach in the history of the industry and demonstrates how the health care sector is becoming an increasingly attractive target for hackers. According to the Office for Civil Rights at the Department of Health and Human Services, the number of breaches which involve more than 500 patients has increased from 13 in 2008 to 256 in 2013 (Anonymous, 2015). The total number of patients affected by such privacy breaches increased from about half a million people in 2008 to nearly nine million people in 2014.

Security experts point to healthcare records as a primary threat vector in 2015 (Arellano, 2014). Interviews at regional hospitals in the central Virginia area reveal continuing threats to those organizations. These organizations face a multitude of attacks on a daily basis. Of course, regulating agencies are aware of the threats to privacy. The Health Insurance Portability and Accountability Act (HIPAA) was passed in 1996. The bulk of the legislation is aimed at availability of health insurance but part of it deals with privacy and security. The privacy portion deals with how insurance companies and other entities that deal with health related data protect that data. This does not address unauthorized access. The security portion however does specifically lay out a set of standards for safeguarding health related data. These standards include administrative safeguards such as maintaining a written policy, security training, contingency plans, internal audits, and procedures for addressing and responding to breaches. They also include physical safeguards such as controlling introduction and removal of hardware and software, access to equipment and hardware, access control, and workstation use. Finally, they include technical safeguards which include protection from intrusion, data corroboration, authentication, and risk management programs.

Though organizations may make a best effort to adhere to the HIPAA guidelines, breaches still occur on a regular basis. There is a large amount of research that examines why this happens (Lapke, 2010). This is outside of the scope of this particular study however. It is not the intent of the paper to analyze why these breaches happen but rather the attitudes of healthcare professionals towards the privacy of healthcare information.

In this paper, we argue that healthcare providers place a high importance on privacy concerns with regards to healthcare information. This argument is based on several factors. The potential for significant HIPAA fines, malpractice lawsuits, and damaged reputations all provide a significant incentive to view privacy as a primary concern for healthcare providers. Healthcare Also, organizations have been slow to adopt the digitization of medical records. This could be demonstrative of unease with illicit remote accessibility of digital records. Also, healthcare practitioners and administrators are much more aware of the breaches that have happened within their field. It is likely that the stakeholders are leery of investigations by governmental agencies or lawsuits by impacted patients should a breach occur.

Literature Review

Privacy in Information Systems research has been explored considerably over the last 30 years. Meldman (1981) discussed the expectations of privacy in the then emerging reality of the information age. Even 30 years ago, the concept of the changing social structures brought on by the increasingly rapid exchange of digitized information was deeply concerning to the public. What is most interesting about this research is that concerns about health related data fell at the very bottom of the list, beneath the likes of the census bureau, the IRS, local police, and the telephone company.

In describing the four ethical issues for the Information Age, Mason (1986) included privacy as a top issue. At the time of publication, the “Information Age” was relatively new however the challenges it

presented were not far from discussion. Information Technology was plainly charged with a force that threatened privacy. We are seeing this concern arise again with the contemporary push for Information Technology in Healthcare Systems.

As noted by Agarwal, et al (2010), this is a remarkable time for Information Systems researchers, as the United States expends extraordinary efforts toward the digitization of its health-care system, and as policy makers across the globe look to information technology (IT) as a means of making health-care systems safer, more affordable, and more accessible. Indeed, much of the research is exploratory in nature and is laying the framework for future, in depth studies. Goldschmidt (2005) evaluated the advantages and risks associated with electronic health care records. It was noted that healthcare lags behind other industries in IT adoption by 15 years. The benefits of a shift to electronic health records include reduced expenses, easier information sharing, reduced office visits, more accurate clinical data, immediate access and instant updates, and a reduction in medical mistakes. The downsides were described as overwhelming complexity of the current system, insurmountable start up costs, and most critically privacy concerns. The greatest concern listed was the security, privacy, and confidentiality of their personal health information. It was described as the potential Achilles' heel of the widespread implementation of digital health records.

This concern was echoed by Hoffman (2009). Privacy in HIT implementation was described as one of the most formidable challenges. Designing HIT that complies with all of the regulations was described as nearly impossible. The inherent complexity of health care delivery is also noted as a privacy-related challenge. With so many entities involved, including hospital administration, caregivers, insurance companies, regulatory agencies, and the like, there are a large number of potential breaches in security.

Quantitatively, as many as 400 people may get a hold of somebody's medical information through the general care process (Cannoy & Salam, 2010). In contrast with the quantitative data described earlier (Greenberg, 2010), Cannoy and Salam (2010) present qualitative data that shows patients uncomfortable with information sharing between hospitals, doctors, specialists, and insurance companies. Furthermore, they did not trust their health plan or hospital to protect their information.

As a final contemporary perspective of consumer's expectations of privacy with healthcare information, Agarwal and Anderson (2011) described a more nuanced and subtle situation. They found health consumers to have a complex perspective driven primarily by emotion. With health issues being closely tied to emotional response, particularly with life changing concerns such as cancer, HIV, or debilitating illness, people make choices in the heat of the moment. This overrides a deliberative cognitive evaluation and clouds decision making. This emotion has a direct impact on patient's willingness to disclose information in various health related settings. The impact of emotion on privacy was reflected in other research (Applebaum, 2002).

The majority of the research reviewed leaned heavily towards the patient's perspectives of privacy with digital health information. The few studies that did mention the other side of the healthcare aisle, mentioned it as an aside and not a focus of the study. This study intends to bridge the gap in the literature. From a practitioner's perspective, this is important because it can inform a critical area in the HIT arena that has been neglected in the past.

Theory

The theory that drives this research is rooted in studies in privacy. No predominant theoretical perspective has emerged to account for the psychological mechanisms guiding employee attitudes and behaviors about workplace privacy (Stanton, 2002). In response to this, a new theory for privacy was developed using Petronio's (1991) theory of communications boundary management (CBM). This originating theory argues that human relationships have an inherent tension between the need for autonomy and the need for intimacy. Intimacy allows one to know another while autonomy helps protect the self from others.

CBM further argues that people balance this tension by negotiating mental boundaries between themselves and those with whom they communicate (Petronio, 1991). This unspoken boundary, or psychological contract, opens for information exchange and closes to restrict the flow. Open boundaries encourage greater information exchange while closes boundaries dampen such exchanges. Stanton (2002) remarked that the elements of CBM overlap with social psychologist's definitions of trust.

As CBM focuses on interpersonal communication, Stanton (2002) sought to modify it to apply in an organizational setting. By synthesizing CBM with a group-value approach to organizational justice (Alder, 1998; Alder & Tompkins, 1997), and a general expectancy-valence framework for privacy protection (Stone & Stone, 1990), a new theory emerged. Like CBM, Information Boundary Theory (IBT), "predicts that motivation to reveal or withhold valued information via a given medium follows rules for boundary opening and boundary closure" (Stanton, 2002, p. 154).

IBT sees the opening and closing of these boundaries to be based more on the expectation of benefits by either receiving/sending or closing off information exchange within an organizational setting. These benefits are categorized in four dimensions: Exoteric, Political, Redemptive, and Protective (Stanton & Stam, 2003). This will form the basis for the theoretical framework to be used in this study. The four dimensions will be cross referenced with the major stakeholders in care giving organizations to analyze their perceptions of privacy in the emerging digital reality. These include doctors, hospital administrators, nurses, and support staff. See table 1:

	Increase Gain	Decrease Loss
Withhold	Political	Protective
Reveal	Exoteric	Redemptive

Table 1: Information Boundary Theory

The four constructs in this Theory leads to four research questions to gauge the attitudes of healthcare providers towards privacy. The first two involve their willingness to reveal information. Do healthcare providers feel it is best to reveal information in order to increase positive outcomes? Also, do healthcare providers feel it is best to reveal information in order to decrease negative outcomes? If it is the case that they feel that revealing information is best for either of these dimensions, then privacy is not a primary concern. The second two involve their desire to withhold information. Do healthcare providers feel it is best to withhold information in order to increase positive outcomes? Also, do healthcare providers feel it is best to withhold information in order to decrease negative outcomes? With this dimension, their agreement that withholding is ideal would demonstrate that privacy is a primary concern.

Survey Design

With IBT forming the basis, we developed a survey to measure the Theory's constructs within the context and setting of Healthcare and more specifically HIT. The four constructs within the Theory (Exoteric, Political, Redemptive, and Protective) all describe different facets of attitudes towards privacy. The Exoteric dimension describes a decision to reveal information in an effort to achieve gains. A person who reveals information does not value the privacy of that information. Within the context of healthcare, the Exoteric dimension would involve improving quality of care, improving patient outcomes, and increasing the ease and efficiency of the job.

Like the Exoteric dimension, the Redemptive dimension is concerned with motivations to reveal information. The driving force to reveal information involves preventing or mitigating loss instead of achieving gains. There are two major aspects within healthcare to consider with regards to minimizing

loss. One is on the financial side and involves insulating the provider from malpractice lawsuits. The second aspect is minimizing errors with the actual care provided.

The Political and Protective dimensions of the Theory involve withholding information. A person who withholds information values the privacy of that information. The first of these, the Political dimension, describes the decision to withhold information in an effort to achieve gains. In the healthcare setting, this would involve provider/administrative conflict and clinical decision making autonomy. The second withholding construct is Protective and this involves withholding information in an effort to prevent or mitigate loss. Within healthcare, this would consist of avoiding litigious outcomes and negative patient outcomes.

These four constructs that make up IBT laid the foundation for our analysis of the attitudes of privacy of healthcare professionals. We developed survey items to capture the various aspects of each construct as they relate to the healthcare realm. These survey items can be seen in Table 2 below.

Theoretical Construct	**Questionnaire Item**
1) Exoteric Revealing Information in an effort to achieve or solidify gains	1.1) Centralized, shared digital healthcare data augments the performance of health care providers
	1.2) Centralized, shared digital healthcare data improves patient outcomes
	1.3) My job is (or would be) made easier by having all stakeholders (including clinicians, administrators, and patients) have access to the same healthcare information
	1.4) My workload is (or would be) more efficient by having all stakeholders (including clinicians, administrators, and patients) have access to the same healthcare information
2) Political Withholding information in an effort to achieve or solidify gains	2.1) My professional risks as a health care provider are increased when administrators or other clinicians have access to my patient's records.
	2.2) I have less professional autonomy when others have access to my patients' records
	2.3) Sharing medical information electronically across all stakeholders leads to increased conflict between administrative requirements and clinical decision making
	2.4) Knowing medical information is shared across all stakeholders, I am more inclined to make decisions that follow administrative requirements rather than follow my best professional judgment
3) Redemptive Revealing Information in an effort to prevent or mitigate loss	3.1) Having medical information shared across all stakeholders will provide an added measure of protection against malpractice lawsuits
	3.2) I have encountered situations where a centralized database of patient information did or would have improved a patient's outcome
	3.3) Centralized, shared digital healthcare data reduces the number of errors made by health care providers
4) Protective Withholding information in an effort to prevent or mitigate loss	4.1) Sharing of medical information across all stakeholders increases my risk of malpractice lawsuits
	4.2) I am reticent to share medical information across all stakeholders unless compelled for fear of malpractice lawsuits
	4.3) Total information sharing will reduce personal engagement between healthcare providers and patients
	4.4) Total information sharing will narrow the dimensions on which healthcare providers are evaluated and compared
	4.5) Total information sharing will reduce the human dimensions of healthcare service

Table 2: Theory Constructs and Related Survey Items

Because the measures of the usage dependent variable are newly created items, we computed the linear composite scores based on the summated mean values of the items (Rai & Patnayakuni, 1996). Specifically, we computed the mean of the usage items and then used this mean score as a formative indicator for the usage dependent variable (Rai & Patnayakuni, 1996). Then, we evaluated the measurement properties of the reflective constructs. Accordingly, we assessed scale reliability, convergent validity, and discriminant validity for all the constructs in the Theory. These measurement properties, however, are not necessary requirements for formative constructs (Diamantopoulos & Winklhofer, 2001).

To ensure adequate convergent validity, all item loadings (outer loadings) should be greater than 0.7, indicating that more than half of the variance is captured by the constructs (Agarwal & Karahana, 2000; Bassellier & Benbasat, 2004). Table 2 presents the items used for the theory testing; all item loadings are greater than or close to 0.7. As suggested by Gefen and Straub (2000), we also verified that the t-statistic for each item loading is greater than 1.96. A further test of convergent validity is to ensure that constructs have an average variance extracted (AVE) greater than or equal to 0.5, implying that 50 percent or more of the indicator variable is accounted for by the latent variable (Chin, 1998). All reflective constructs meet this requirement.

	EXOTERIC	POLITICAL	PROTECT	REDEM
EXOT1	**0.79**	-0.30	-0.35	0.43
EXOT2	**0.74**	-0.22	-0.38	0.61
EXOT3	**0.87**	-0.52	-0.41	0.46
EXOT4	**0.81**	-0.30	-0.24	0.41
POLGN1	-0.23	**0.68**	0.42	-0.10
POLGN2	-0.31	**0.84**	0.54	-0.14
POLGN3	-0.41	**0.81**	0.47	-0.23
POLGN4	-0.35	**0.70**	0.48	-0.11
PROTW1	-0.39	0.51	**0.73**	-0.35
PROTW2	-0.21	0.60	**0.70**	-0.17
PROTW3	-0.30	0.34	**0.80**	-0.27
PROTW4	-0.24	0.52	**0.73**	-0.18
PROTW5	-0.31	0.44	**0.76**	-0.31
REDEM1	0.33	-0.08	-0.23	**0.66**
REDEM2	0.25	-0.16	-0.27	**0.74**
REDEM3	0.63	-0.19	-0.29	**0.79**

Table 3: Crossloadings of Survey Items

We assessed discriminant validity in two ways. First, we ensured that each item loaded more strongly on its target construct than on any other construct in the model (Fornell & Larker, 1981). As shown in Table 3, all items meet this requirement. Second, we checked whether the square root of the AVE for each construct was larger than its correlation with any other construct (Fornell & Larker, 1981). As shown in Table 4, all constructs meet this requirement. Scale reliability was assessed for constructs with more than one item via Cronbach's alpha and composite reliability (Fornell & Larker, 1981). As shown in Table 4, the Cronbach's alpha and composite reliability scores for all reflective constructs exceed the recommended .7 cutoff (Nunnally, 1978).

	AVE	Composite Reliability	Cronbachs Alpha
EXOTERIC	0.51	0.86	0.81
POLITICAL	0.58	0.84	0.76
PROTECT	0.55	0.86	0.80
REDEM	0.54	0.78	0.57

Table 4: Assessing Validity

Data Gathering and Demographics

The data was collected between May and November of 2013. Several attempts were made in the early months to gather data by way of broad marketing. The Primary Investigator made contact with the Director for Health and Human Services for the state he resided in. The Director suggested sending him an introductory email that called for participation in the survey. He would then send this email on to the three main medical associations in the state. He felt that if the email came from him, it would be more likely to be read and acted on. There were approximately 25,000 members of these various associations. Two months after this action, 23 healthcare professionals had responded.

After the disappointing response and further discussions with the Director, it was determined that this method would not yield further success. Doctors, nurses, and hospital administrators are inundated with generic requests to complete surveys and they ignore most if not all of these requests. SurveyMonkey indicated that they could return the required 100-200 responses for the a fee of $10,000.

Because $10,000 was not in the research budget, the PI decided to act directly in his regional area. He sent personal requests for participation to 327 healthcare professionals in three surrounding hospitals, eight private practices, four specialty clinics, and five treatment facilities. Of these 327 requests, 148 subjects responded. This yielded a response rate of 45%.

The demographics of the respondents showed that the majority (79%) were Caucasian, with Hispanic, African American, and Asian evenly distributed among the remaining 21%. This is reflective of the racial demographics of the regional area. The majority (68%) of respondents were also female. There were roughly equal groupings of age ranges with 20-30, 31-40, 41-50, and 51-60 each occupying about 22% of the respondents. Older respondents (>61 years) and younger (<20 years) respondents each had smaller percentages. Approximately 70% of the respondents had either a Bachelor's Degree, Master's Degree, Professional Degree, or Doctorate Degree. The practice area was broadly distributed as can be seen in Figure 1 below.

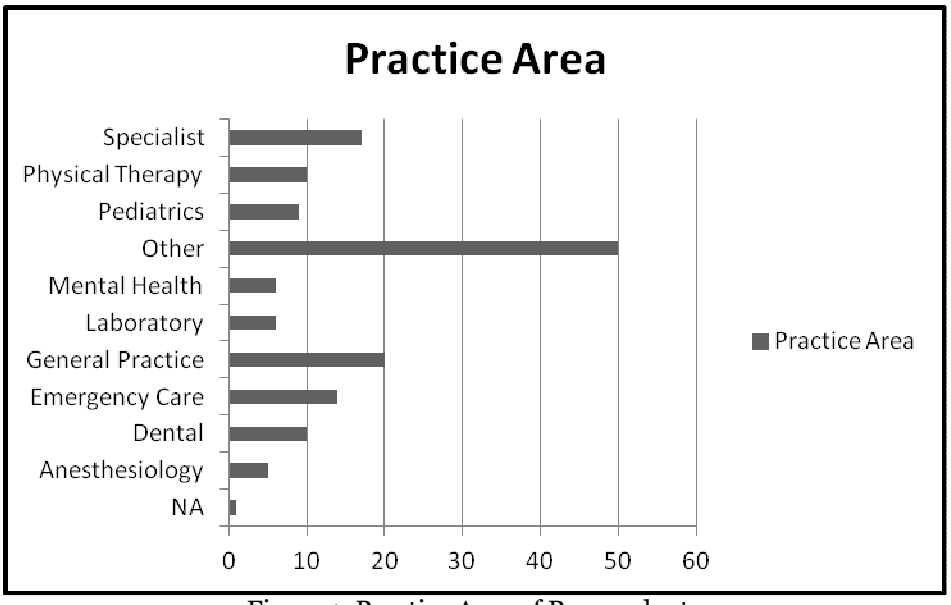

Figure 1: Practice Area of Respondents

Analysis

The analysis involved hypothesis testing for each of the four dimensions of IBT. The survey analysis is based on a total of n=148 responses. Each survey item was coded on a 7-point Likert scale where 1 designates "Strongly Disagree", 4 designates "Neutral", and 7 designates "Strongly Agree". For the Exoteric and Redemptive dimensions, it was hypothesized that the respondents would tend more toward disagreement than toward neutrality or disagreement. For the Political and Protective dimensions, it was hypothesized that the respondents would tend more toward agreement than toward neutrality or disagreement.

As was stated in the introduction, we are arguing in this paper that privacy is a primary concern of healthcare professionals. In order to support this argument, it is hypothesized that respondents would not agree with revealing information. It is also hypothesized that they would agree with withholding information. Accordingly, a hypothesis test of the following form was performed on the response means for each dimension of the Theory:

Hypothesis 1: $\mu<4$ for the Exoteric Dimension
Hypothesis 2: $\mu<4$ for the Redemptive Dimension
Hypothesis 3: $\mu>4$ for the Political Dimension
Hypothesis 4: $\mu>4$ for the Protective Dimension

Mean responses ranged from a low of 2.92 to a high of 6.1. For each hypothesis pair a T-test was performed at $\alpha=0.05$. The significance threshold was set at .05. It was found that the respondents were in agreement with the Exoteric dimension. That is to say that they agreed with the decision to reveal information in an effort to achieve gains. They were also in agreement with the Redemptive dimension. This refers to the construct of revealing information for the purpose of mitigating loss. The respondents were in disagreement with the Political dimension. They did not agree with decisions that involve withholding information in order to achieve gains. Finally, they also disagreed with the Protective dimension. That is to say that they disagreed with decisions to withhold information in order to prevent or mitigate loss. The results are shown in Table 5 below:

	Mean	StDev	P-Val (T-Test)
Exoteric (revealing)	5.547	1.166	$p < .001$
Redemptive (revealing)	4.939	1.142	$p < .001$
Political (withholding)	3.421	1.391	$p < .001$
Protective (withholding)	3.318	1.302	$p < .001$

Table 5: Survey Results

The results did not support any of the hypotheses. The Exoteric and Redemptive dimensions both showed a strong tendency for healthcare professionals to reveal information. The Political and Protective dimensions showed reluctance to withhold information. The desire to minimize litigation and maximize patient outcomes appears to hold sway over the need to keep data private.

Conclusion

This paper revealed some surprising results regarding healthcare providers' perceptions and expectations for privacy of data in HIT systems. Given the potential for significant HIPAA fines, lawsuits, and reputation damage, we felt it was very likely that healthcare professionals would place a high priority on privacy. This argument was conceptualized in a survey based on Information Boundary Theory. This Theory allowed us to examine the four main dimensions of attitudes towards privacy. Is someone motivated to reveal or withhold information? Does this motivation stem from a need to achieve gains or prevent loss?

The respondents unexpectedly showed a strong willingness to reveal information. They also showed little desire to withhold information. This is not to say that healthcare professionals do not care about privacy. The regulatory, litigious, and personal motivations to maintain patient confidentiality are all still very real elements that these professionals face on a daily basis. However, it is clear that healthcare professionals put personal and organization gain as well as mitigating personal and organizational loss over privacy.

That major breaches continue to happen despite regulatory and litigious ramifications likely means one of two things: healthcare professionals and the Information Systems professionals that support them are incompetent or they do not prioritize privacy. Given the degree of education and preparation that these parties have, incompetence is not likely. It only makes sense that putting patient outcomes above all else is their main priority. Unfortunately, this leaves the real problem of data breaches unsolved.

The contributions of this research are both theoretical and practical. The theoretical contribution lies with the study's application of privacy theory to HIT research. As previously stated, no predominant theoretical perspective has emerged to account for the psychological mechanisms guiding employee attitudes and behaviors about workplace privacy (Stanton, 2002). In response to this, a new theory for privacy, Information Boundary Theory, was developed. The constructs in IBT provided the framework for the survey created and used in this research.

The practical contribution comes from the fact that the research informs practitioners of an oft overlooked topic that is vital to the continued success of healthcare organizations. The research found that practitioners are primarily concerned with patient outcomes. Where the data is stored and whether or not its privacy protected is of little consequence to healthcare providers. This research illustrates the danger of this perspective for the practitioner. The regulatory, litigious, and reputation damaging outcomes of data breaches cannot be overstated.

Limitations of this research come mostly from its limited population of respondents. Given the difficulty in locating healthcare providers willing to participate at the state level is indicative of the likely response rate at a national scale. The statistical generalizability of the results is limited in that the respondents might be demonstrating a regional bias that is not reflective of national perspectives. A researcher with

the resources to obtain a nationally representative sample could replicate this study to determine if the regional bias is an issue.

Future research plans include an in depth qualitative case study in a hospital setting. Obtaining a more in depth analysis could prove insightful for a thorough analysis of the Achilles heel of HIT. As stated in the limitations, another potential direction for future research could include a more broad reaching survey to determine if the regional results discussed in this paper are mirrored nationally. Implementing HIT on a grand scope will happen one way or the other over the next several years and protecting the sensitive information of those at risk will help ensure its success.

References

Agarwal, R., & Anderson, C. 2011. *The Complexity of Consumer Willingness to Disclose Personal Information: Unraveling Health Information Privacy Concerns*. Paper presented at the eHealth Initiative's 5th Annual Conference.

Agarwal, R., Gao, G., DesRoches, C., & Jha, A. 2010. The Digital Transformation of Healthcare: Current Status and the Road Ahead. *Information Systems Research,* 21(4).

Agarwal, R., & Karahana, E. 2000. Time flies when you're having fun: Cognitive absorption and beliefs about information technology usage. *MIS Quarterly,* 24(4), 665-694.

Alder, G. 1998. Ethical issues in electronic performance monitoring: a consideration of deontological and teleological perspectives. *Journal of Business Ethics,* 17, 729-743.

Alder, G., & Tompkins, P. 1997. Electronic performance monitoring: an organizational justice and concertive control perspective. *Management Communication Quarterly,* 10, 259-288.

Anonymous. 2015. *Breaches Affecting 500 or More Individuals*. Retrieved. from https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

Applebaum, P. S. 2002. Privacy in Psychiatric Treatment: Threats and Response. *American Journal of Psychiatry,* 159, 1809-1818.

Arellano, N. 2014. Top 9 Security Threats to Prepare for in 2015. Retrieved 01/28/2015, 2015, from http://www.itworldcanada.com/slideshow/top-9-security-threats-to-prepare-for-in-2015

Bassellier, G., & Benbasat, I. 2004. Business competence of information technology professionals: Conceptual development and influence on IT-business partnerships. *MIS Quarterly,* 28(4), 673-694.

Cannoy, S., & Salam, A. 2010. A Framework for Health Care Information Assurance Policy and Compliance. *Communications of the ACM,* 53(3).

Chin, W. 1998. The partial least squares approach for structural equation modeling. In G. A. Marcoulides (Ed.), *Modern methods for business research* (pp. 295–336). Hillsdale, NJ: Lawrence Erlbaum Associates.

Diamantopoulos, A., & Winklhofer, H. 2001. Index construction with formative indicators: an alternative to scale development. *Journal of Marketing Research,* 38(2), 269-277.

Fornell, C., & Larker, D. 1981. Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research,* 18(1), 39-50.

Gefen, D., & Straub, D. 2000. A practical guide to factorial validity using PLS-GRAPH: Tutorial and annotated example. *Communications of the Association for Information Systems,* 16, 91-109.

Goldschmidt, P. 2005. HIT and MIS: Implications of Health Information Technology and Medical Information Systems. *Communications of the ACM,* 48(10).

Greenberg, A. (2010). Health Care's Digital Privacy Debate. *Forbes*.

Hoffmann, L. 2009. Implementing Electronic Medical Records. *Communications of the ACM,* 52(11).

Lapke, M. 2010. *Institutionalization of Information Systems Security Policy at a Large Financial Organization*. Paper presented at the The 9th Security Conference, Las Vegas, NV.

Mason, R. 1986. Four Ethical Issues of the Information Age. *MIS Quarterly,* 10(1), 5-12.

Meldman, J. 1981. *American Expectations of Privacy in an Information Age*. Paper presented at the Fourteenth Annual Hawaii International Conference on Systems Science

Nunnally, J. 1978. *Psychometric theory* (2nd ed.). New York: McGraw-Hill.

Petronio, S. 1991. Communication Boundary Management: A Theoretical Model of Managing Disclosure of Private Information Between Married Couples. *Communication Theory,* 1, 311-335.

Rai, A., & Patnayakuni, R. 1996. A structural model for CASE adoption behavior. *Journal of Management Information Systems,* 13(2), 205-234.

Stanton, J. 2002. Information technology and privacy: A boundary management perspective. In S. Clarke, E. Coakes, G. Hunter & A. Wenn (Eds.), *Socio-Technical and Human Cognition Elements of Information Systems*. London: Idea Group.

Stanton, J., & Stam, K. 2003. Information Technology, Privacy, and Power within Organizations: a view from Boundary Theory and Social Exchange perspectives. *Surveillance & Society,* 1(2), 152-190.

Stone, E., & Stone, D. 1990. Privacy in organizations: theoretical issues, research findings and protection mechanisms. *Research in Personnel and Human Resources Management,* 8, 349-411.