6-2015

Patient Perception of Privacy and the Role of Electronic Medical Records

Max Louis Willinger

Union College - Schenectady, NY

Follow this and additional works at: https://digitalworks.union.edu/theses

 Part of the Health and Medical Administration Commons

Patient Perception of Privacy

and the Role of Electronic Medical Records

By

Max Louis Willinger

****

Submitted in partial fulfillment

Of the requirements for

Honors in the Department of Sociology

UNION COLLEGE

March 2015

ABSTRACT

WILLINGER, MAX L. Patient Perception of Privacy and the Role of Electronic Medical Records

    Department of Sociology – March 2015.

ADVISOR: Professor Timothy Stablein

In order to better manage patient records, hospitals and health care settings across the nation have begun to implement electronic medical record systems (EMR). The purpose of this transition is to reduce excessive amounts of paper, to decrease administrative costs, and to increase the overall quality of care. With the implementation of the EMR, relationships between physicians and their patients have the potential to change. Research has shown that patient perceptions are changing regarding confidentiality, trust, and privacy in the doctor-patient relationship because of patient medical records being stored electronically as opposed to being locked away in a file cabinet. Building on these findings, I analyze in-depth interviews of patients (N=44) to explore patient perceptions of EMRs and Privacy. The purpose of this research is to discover how patients perceive EMR, how they perceive privacy, and how they think the EMR plays a role in that privacy perception. I found two types of trust that have arisen due to EMR implementation, interpersonal trust and institutional trust. These types of trust are involved with providing the foundation for the formation of privacy perceptions. When patients are not concerned with the inappropriate exposure of their personal health information and perceive that the privacy of their records stored in the EMR is being adequately protected, they are much more likely to perceive trust and privacy with their physician and/or within their health care setting, and will be more likely to disclose their personal health information, which will lead to better patient care.

ACKNOWLEGDEMENTS

Firstly, I would like to take this opportunity to thank Professor Timothy Stablein. I am very grateful that he invited me to work with him on analyzing the research that he and his team had collected. I also want to thank him for his guidance and support throughout this entire project because without him, this thesis would not have been possible.

I would also like to take this opportunity to thank my second reader and Sociology advisor, Professor Melinda Goldner, for her endless support throughout my four years here at Union. She was one of my first and will be one of my last professors, and is responsible for introducing me to the field of sociology, and for that, I am grateful.

Lastly, I would like to thank my entire extended family, especially my parents, for always believing in me and supporting me through my various endeavors. I have always appreciated having such a close family; they have helped shape me into the man I am today.

TABLE OF CONTENTS

Chapter 1

Introduction

  With the implementation of the Patient Protection and Affordable Care Act (ACA),

millions of uninsured Americans gained health insurance, which meant that health care

institutions would soon be receiving an influx of new patients seeking care. This increase in

patient population means that more patients will be seen by more health care professionals;

therefore, it is of extreme importance that the patient's care is coordinated well amongst each of

the providers caring for that patient. The ACA also gave rise to a new concept of Accountable

Care Organizations (ACOs), which are organizations consisting of a variety of providers that a

patient has access to. If a patient sees his cardiologist and then subsequently visits his primary

care physician, the patient would expect that all information obtained by his or her cardiologist

would be available to his or her primary care physician, otherwise potentially important

information obtained by the cardiologist would remain unknown to the primary care physician

and medical error may result. Sharing patient information has become much easier because of

the ACA due to the nation-wide implementation of electronic medical record (EMR) systems.

However, as important and influential as these medical technologies may seem, there are many

problems can occur when dealing with medical information in an online system.

  The concept of confidentiality in medicine can be dated all the way back to 400 B.C. to

the Hippocratic Oath. The Hippocratic Oath outlined how a medical professional should act, and

is still sworn today by those who are about to enter the medical profession. With the transition

from paper records to electronic records, personal health information becomes much more

readily accessible and raises issues with the confidentiality of the information stored in those electronic systems.

Since the implementation of the ACA, the United States has been experiencing large-scale changes that affect the way health care is provided to patients, specifically in terms of health information technology; this is why studying the implementation of EMR is so important. The goal of the EMR was to decrease cost and increase quality of care, which would ideally lead to better patient outcomes. However, this new technology poses some interesting changes in the way patients perceive their privacy. If patients neither trust their doctors, nor believe that their medical information is private and confidential, they will not be completely honest with their providers, which can lead to serious of issues including medical error. Some favor and some are worried about the implementation of the EMR, but with the advent of this new technology, it seems as though confidentiality and privacy have become implicated.

In this thesis, I explore patient perceptions of privacy of their medical information and the role that the implementation of electronic medical records plays in the formation of those perceptions. I also explore how patients perceive the major benefits and problems associated with EMR, how EMR affects doctor-patient relationships and the expectation of privacy and trust in those relationships, the importance of privacy and confidentiality of their medical information, the meaning of privacy in relation to medical records specifically and the differences in privacy between paper and electronic records, who is responsible for maintaining said privacy, and how much control the patient has in the protection of their information.

The rest of Chapter 1 reviews literature about patients perceptions of privacy, confidentiality, and trust in the health care system and then specifically in terms of EMR.

Chapter 2 explains the methods by which the data were collected and analyzed; the data consist of patient interviews in two hospitals in the northeastern region of the United States. Chapter 3 reports the findings of the interview data regarding patients perceptions of privacy, confidentiality, and trust, and the role that the EMR plays in the formation of those perceptions, and Chapter 4 will discuss those findings.

Privacy, Confidentiality, and Trust in Health Care

The Hippocratic Oath is an oath sworn by all medical students that outlines the ethical standards that are expected to be upheld while practicing medicine. One of the most important ethical principles discussed in the ancient oath is that of confidentiality. According to one of the most widely accepted translations of the original oath, the confidentiality clause reads, "And about whatever I may see or hear in treatment, or even without treatment, in the life of human beings — things that should not ever be blurted out outside — I will remain silent, holding such things to be unutterable [sacred, not to be divulged]…" (Von Staden 1996: 407). The Hippocratic Oath included this clause to portray the importance of confidentiality in the treatment of patients, and that such patient information is "unutterable" and "sacred". The Hippocratic Oath was written around 400 B.C. and is still used today; however, as time progressed, other codes of ethics were developed, many of which included similar clauses about patient confidentiality.

In 18th century Scotland, the Edinburgh Oath was developed and pledged by the students of the University of Edinburgh Medical School. Its mention of confidentiality read, "And lastly, never, without great cause, to divulge anything that ought to be concealed, which may be heard or seen during professional attendance…" which differs slightly from that of the Hippocratic

Oath (Baker 2013: 58). This oath adds the phrase "without great cause" which leads to the question, what defines great cause? Although every medical student at Edinburgh swore the oath, there have been many documented incidents where confidentiality was clearly breached. In the eighteenth century, it was relatively common for physicians to engage in flytes, which were verbal duels with the goal of publicly disrespecting a rival physician in order to proclaim one's status and honor (Baker 2013: 88). This verbal dispute generally involved the divulging of patient information, which went directly against the confidentiality clause of the oath that they had pledged. Lo and behold, physicians were not abiding by the oath that they had previously sworn. As more codes of ethics were developed, the confidentiality clauses changed a bit, but the central idea remained – do not under any circumstance divulge any information regarding one's patients. Today, medical students pledge a rendition of the Hippocratic Oath upon entering medical school with the goal that its principles and clauses will be upheld in practice, especially that of patient confidentiality.

    As similar as the concepts of confidentiality and privacy may seem, they are not the same. Privacy is when one is free from intrusion, whereas confidentiality is when information is limited to only the appropriate viewers (Davis et al. 1999). In other words, if someone spies on you and sees you walk into a clinic, your privacy is being violated, but if a health care worker in that clinic decides to send your medical records to a news source without your permission, your medical record confidentiality is violated (Davis et al. 1999). In essence, privacy refers to an individual's ability to control the accessibility to his or her medical records (Cantor 2006). Understanding this difference is important in understanding how and why patients have different perceptions of what encompasses their privacy. Specifically in health care, privacy concerns the

responsibility of the health care providers to protect their patients and their patients' records

from any sort of disclosure to anyone unauthorized to see the records (Davis et al. 1999). The

range of interpretations as to exactly what the health care worker's responsibilities are in terms of

protecting patients' privacy is so wide, demonstrating the need to understand patients'

perceptions of that privacy.

When not worried about public exposure, patients were found to give more accurate

information, and more accurate information can lead to more effective treatment and better

patient outcomes (Sankar et al. 2003). Public exposure can be anything from someone other than

the patient's physician viewing the patient's medical information, to a member of the community

seeing the patient enter a community clinic. In their study, Sankar et al. (2003) analyzed a

compilation of research involving patient views on confidentiality. They found that patients

seemed to be unclear as to the basic purpose of the confidentiality leading many to overestimate

and underestimate how their confidentiality is protected (Sankar et al. 2003). Some patients even

reported signing release-of-information forms because they were either under the impression that

they had no choice or they had not realized what they had signed (Sankar et al. 2003). This lack

of understanding stems from a lack of trust in confidentiality protection mechanisms, and has led

patients to deny or forgo medical treatment that may have been necessary to restore their health.

Another study showed that 85% of patients reported that they trusted the practices of their

health care system, but they were overall unaware, misinformed, and confused about data sharing

practices, thinking that there was less sharing than actually took place (Goodwin et al. 2002). By

trusting the "practices" of their health care system, patients are trusting the institution

(institutional trust); however, another form of trust is equally, if not more, important than

institutional trust, and that is interpersonal trust — trust between the patient and the caregiver. By educating patients and making them aware of the confidentially that is practiced by health care workers, interpersonal trust will increase leading to an increase in institutional trust, and patients will be more likely to seek the care they need. In order to do so, patients may desire more control in what is kept confident and private and what can be shared with others.

In a 2012 study conducted by Caine and Hanania, patients were asked who they trusted sharing their medical information with. When the patients were provided with a list of different types of health care providers in which they felt comfortable sharing their medical information with, not one reported feeling comfortable with sharing all of their information with any single provider (Caine and Hanania 2012). That being said, there was a clear difference between the sharing of what was deemed less sensitive material with what was deemed more sensitive material. Patients were more likely to share less sensitive material, which was anything not defined by the National Committee on Vital and Health Statistics as more sensitive information. More sensitive information included domestic violence, genetic information, mental health, sexual information including sexually-transmitted diseases, and substance abuse (Caine and Hanania 2012). These patients only wanted their information to be shared if they thought it would somehow benefit their health, otherwise they preferred their medical records to be private (Caine and Hanania 2012). Other studies have shown similar patterns in patient distrust with the privacy of their medical information. In a California high school, more than half of the students surveyed did not trust that their doctors would keep a sexually-transmitted disease secret from their parents although they knew that every physician pledged an oath of confidentiality upon entering the medical profession (Sankar et al. 2003).

Understanding the privacy and confidentiality aspects of health care is crucial, but it is having trust in the system as a whole that is of the utmost importance. When trust is referred to in the context of health, it is usually uncertain whether that trust is referring to a physician or another medical professional, a hospital or other medical institution, or the profession as a whole (Brownlie 2008). Trust can be defined as the expectation that medical professionals and medical institutions will meet the responsibilities to their patients (Mechanic 1998). Studies have shown that although the public tends to trust their doctors, they tend to highly distrust health care systems, which may be due in part to the privatization of medical care, growth of managed care, and technological growth (Dew et al. 2007; Mechanic 1998). Other studies have portrayed the lack of trust that patients have in their physicians. With the increasing growth of personal autonomy, patients are less likely to simply accept everything that their doctors may tell them, portraying the shift away from the paternalistic behavior that was common years ago (Mechanic 1998). With the advent of sources such as WebMD®, patients are becoming more knowledgable about their health, and therefore seek more control over their medical care and the manner in which they receive that care. This increase in knowledge seen in patients is leading to the trend of patient-centered decision-making models that are being implemented by institutions today, which aim at reducing the paternalistic nature of the doctor-patient relationship and increasing patient autonomy (Mechanic 1998). Patient trust in his or her physician is the foundation of the doctor-patient relationship. Consultation and compliance become compromised, and the doctor-patient relationship becomes meaningless without trust (Dew et al. 2007; Hall et al. 2001).

Accounting for trust in the field of medicine is especially important today because it can be used as a performance measure in the pay-for-performance model of reimbursement. Trust

measures can also help to determine and improve the key aspects of the doctor-patient

relationship (Hall et al. 2002). For example, in his 1998 study, Mechanic outlines and defines

five dimensions of trust: "(1) expectations about physician's competence, (2) the extent to which

doctors are concerned with their patients' welfare, (3) physician control over decision making,

(4) physicians' management of confidential information, and (5) physicians' openness in

providing and receiving information" (Mechanic 1998: 663-664). It is rare that those who see a

physician believe that he or she is incompetent because since its beginnings, the medical

profession has conveyed the notion that doctors, no matter who, could provide competent service

(Mechanic 1998). This is because the field of medicine is known to be highly academically

competitive, medical training is careful and requires serious talent, and entrance to the profession

is highly controlled. It would seem as though trusting the physicians and the profession should be

the obvious thing to do; however, not all physicians are alike. Doctors are taught how to record a

patient's history during their medical training, but they may not act exactly in the way they were

trained, which can lead a patient to perceive incompetence. Not just while recording patient

history, but physicians may be also perceived as incompetent while performing a physical exam

or communicating important sensitive information (Mechanic 1998), and research has shown that

when patients don't trust their doctors, they may lose trust in their institutions and their health

plans associated with their physicians (Dew et al. 2007; Hall et al. 2001).

It doesn't take much in order for a physician to develop a foundation of trust with a

patient. According to Mechanic (1998), listening intently, asking pertinent questions, and

maintaining eye contact while dealing with a patient has been known to lead to a more

trustworthy doctor-patient relationship. As they familiarize themselves with their patients,

physicians start to gauge how much or how little information their patients want to hear; however, research has shown that doctors tend to underestimate and tend to not provide enough (Mechanic 1998).

On the contrary, if patients do not have full trust in their physicians, they may be hesitant in telling their physicians all of their necessary medical information. If there is a stigma attached with the information resulting in potential embarrassment or if a consolation was rushed and impersonal, patients have been known to keep medical information from their providers (Dew et al. 2007). That being said, when patients disclose personal information, it is expected that the information remain confidential. In this context, it is appropriate for the physician to share the personal information of his or her patient with other members of the medical team involved in the patient's treatment, but where the line becomes gray is when confidential information is shared between other medical personnel, be it insurance company employees, billers, or coders (Mechanic 1998). These personnel are most likely not adequately trained in medical ethics and may inadvertently breach the confidentiality of the information; this is how the movement towards managed care complicates the issue of confidentiality and privacy practices (Mechanic 1998). Along with managed care and the sharing of information amongst various providers, electronic medical records are becoming more common and have the potential to change the way privacy, confidentiality, and trust are understood in the medical context.

Electronic Medical Records, Privacy, Confidentiality, and Trust

Privacy is hard to define due to the fluid nature of its meaning. The concept can be considered fluid because its definition changes as society changes, and the societal change in

health care today involves the transition from paper records to electronic records as health information technology becomes increasingly common. In order to keep paper copies of medical records private, they would be kept in a closed folder and locked away in a file cabinet. With the advent and implementation of the electronic medical record systems, there is neither a folder to close nor a file cabinet to lock; the information is put on a computer system with passwords and firewalls as mechanisms of privacy, which raises the overarching question: *How private is the internet and do you trust it?* Privacy issues don't simply concern patients, but also physicians, especially primary care providers (AlHamad et al. 2014). Electronic medical records allow medical personnel to store and share information using a computer system rather than a paper system (Miller and Tucker 2009). A 2011 study showed that a majority of people were in favor of the use of EMR and believed that the benefits of the EMR outweighed the risks of privacy issues (Gaylin et al. 2011; Pyper et al. 2004). That being said, many patients have reported feeling that the use of EMR actually makes them worry about their privacy.

Trusting this new technology comes hand in hand with trusting that the institution or the hospital that put the technology in place has processes to ensure the competence of the people using the technology (Farquharson and Critchley 2004), and in the case of the EMR, to ensure the security of the information stored in that technology. Trust in online technologies has forever been an issue as new technologies cause social change, and therefore changes in daily life (Zarcadoolas et al. 2013). With the advent of the EMR, a computerized system that is used to access any and all medical records, patients have been concerned about the security of their information. Slowing the trustworthiness of the EMR is that fact that it is a novel technology and with novelty comes the natural unfamiliarity with the system and its capabilities (Nissenbaum

2004). In 2002, the level of comfortability with the overall rate of technological change in the

United States, where zero is not comfortable at all and ten is very comfortable, was reported to

be just under seven, indicating a relative comfortability with technological change (Gilding and

Critchley 2003).

EMR systems have the potential to improve coordination of care and quality of care,

which could in turn decrease hospital costs and lead to better patient outcomes (Caine and

Hanania 2012). The role of EMR is different in the eyes of the hospital than it is in the eyes of

the patient. One of the main purposes of the EMR is to increase the accessibility and sharing of

patient information (Barrows and Clayton 1996). However, with increased sharing of

information comes an increase in the likelihood that someone other than an authorized health

care worker will be able to access private medical information, which is why patients question

the alleged privacy protection that comes along with EMR. That being said, studies have shown

that patients are much more likely to be in favor of and support the health information

technology if they are able to experience its benefits first-hand (Merisalo 2012). In her study,

Merisalo (2012) found that the benefits realized and valued by patients who are under the care of

providers who utilize EMR include the avoidance of having to repeatedly fill out forms regarding

their medical information, and the enhanced ability to share medical information with all of their

providers (Merisalo 2012). The study also found that patients who have online access to their

EMR find benefits in having the control to find and correct errors in their records, and the ability

to understand their health condition better, and keep up with their medications (Merisalo 2012).

Studies have shown that patients want to control the accessibility of their medical records

(Pyper et al. 2004; Caine and Hanania 2012; Mandl et al. 2001). This idea of patients having

direct access to their medical records online is an important health information technological tool and is sometimes referred to as the patient portal (Zarcadoolas et al. 2013). As defined by HealthIT.gov, a patient portal is an "internet application that allows patients to access their electronic health records and communicate with their health care providers" (Zarcadoolas et al. 2013: 168). Patient portals allow patients to increase their autonomy by challenging the traditional top-down methods of health care communication; as opposed to patients simply listening to and believing every word the physician says, patients now have the available information at their fingertips. It is important to also realize that these portals will never replace provider or hospital-based records as providers need their own versions of their patient's medical information for various clinical, financial, and legal reasons (Mandl et al. 2001). That being said, Mandl et al. (2001) claims that there is potential for patient controlled portals to complement the existing data in a hospital or provider-based system, only with the appropriate consent and access privileges.

These portals allow for patients to communicate with their providers, manage their medications, schedule appointments, review test results, and access their medical histories (Zarcadoolas et al. 2013). Because the portals give the patients the ability to fill out necessary medical forms before even coming to the office, it cuts down the waiting time in the office which may in fact increase the amount of patients the doctor sees daily, a win-win situation. Another benefit of the portal system is its ability to increase access to medical information. Many patients have had serious complaints about the lack of time spent with their doctors during visits and the growing complexity of the information given by their providers (Zarcadoolas et al. 2013). Research shows that even if the patients were able to understand and comprehend all of the

information given by their provider during a visit, they would only be able to remember about half of it (Zarcadoolas et al. 2013). The accessibility of health information that comes along with these patient portals allows patients to have a better grasp on their health, allows them to be more proactive in taking care of themselves, and lessens the burden of trying to remember everything from the visit (Zarcadoolas et al. 2013). Zarcadoolas et al. (2013) argues that it is the changing of perceptions regarding EMR that is necessary in order for patients to be able to see these technologies as an extension of the doctor's visit rather than an impediment to the doctor-patient relationship.

These online patient portals give more control and a greater sense of confidence and empowerment to patients (Zarcadoolas et al. 2013). In turn, that empowerment may help in satisfying some of the aforementioned concerns held by patients. This shows that health information technology has the potential to aid patients in the understanding of their medical records and resolve some privacy concerns. However, the online nature of these portals as a form of EMR still leaves room for privacy and security issues to be had by patients (Zarcadoolas et al. 2013; AlHamad et al. 2014). In Merisalo's (2012) study, more than half of the respondents worried that the EMR would lead to more data breaches, and that the adoption of EMR would lead to more personal information being stolen or lost. Zarcadoolas et al. (2013) found that security and privacy concerns were lessened once specific security aspects of the patient portals were discussed and the potential benefits were outlined. AlHamad et al. (2014) found that a lack of control and a lack of sufficient safeguard mechanisms were perceived by patients, so they presented recommendations for managing patient's privacy in the EMRs. These procedures that

plan to protect patient's personal data are crucial in minimizing privacy concerns as any distrust in the system lessens the value perceptions of these systems (AlHamad et al. 2014).

AlHamad et al. (2014) recommended that anyone involved in providing personal information should not disclose anything orally or in writing to any unauthorized personnel including friends, family, and government. Another recommendation involved including in the privacy statement all of the conditions and purposes under which the patient's personal information may be disclosed so that patients are informed before they reveal any information (AlHamad et al. 2014). This is an especially important aspect because if a patient cannot fully account for the privacy of his or her information, he or she would be less likely to tell a provider everything, resulting in the potential nondisclosure of pertinent medical information (Miller and Tucker 2009). AlHamad et al. (2014) also suggested that security measures should be in place that identify how long the data should be kept in the system, i.e. how long patient X's record will be archived until deletion, and how the deletion process would work. General privacy concerns in the realm of internet-based technologies include identity/location disclosure, linking data to other places, and the sense of being monitored (AlHamad et al. 2014).

Electronic medical records should be designed and implemented so that they are able to exchange all stored data according to public standards without any doubt of the private nature of that information (Mandl et al. 2001). Many of the EMR systems in place fragment the medical records by having different means of receiving, processing, storing, and forwarding information, which causes a major issue; all EMR systems should be able to accept data from any number of sources and have it be compatible with their system (Mandl et al. 2001). In order to circumvent

this issue of fragmentation, EMR needs to be universally accessible, able to guard patient's

privacy, and able to be built according to public standards (Mandl et al. 2001).

Other Factors that Influence Health Care Privacy

Health information technology and electronic health information exchanges are crucial

components in the transformation of the health care system today (McGraw et al. 2009). Health

care is on its way in being part of the technological age with the implementation of EMR;

however, this implementation has not exactly addressed the issue of privacy. Countless studies

have shown that the only way to build public trust in health care technologies is to develop and

establish a straight-forward, easy to understand framework of rules and regulations that layout

who has access to information, who can use information, and when disclosure of information is

appropriate (McGraw et al. 2009). In 1996, the United States Congress passed the Health

Insurance Portability and Accountability Act (HIPAA). The rules of this act were the first of its

kind in the protection of health care privacy (McGraw et al. 2009); that being said, there is quite

a variation in the literature in terms of whether HIPAA is adequately addressing privacy

protection in this digital age in which we live.

It is known that few patients actually know what is done with their medical records, and

even less than those few think they have complete control over their records (Annas 2003).

However, a more recent study showed that patients were quite knowledgeable and confident in

regards to HIPAA and its privacy protective mechanisms (Williams et al. 2008). Because of this

shift to EMR, entities outside of the heath care field are now able to handle personal health

information, which becomes an issue because HIPAA's rules and regulations do not apply to

those entities (McGraw et al. 2009). The entities not covered by HIPAA include the health

information exchanges, which are the organizations that handle the collection and dissemination

of personal health information between health care providers/personnel and associated health

plans (McGraw et al. 2009). This is troubling because patients are aware that physicians pledge

an oath involving confidentiality, but patients are also aware of the fact that those who work in

organizations not covered by HIPAA have never taken such a pledge, and confidentiality may not

seem as serious to them as it does to the patients and the physicians.

Another problem with HIPAA's privacy protections is that de-identified health

information is not covered; de-identified health information is any health information that does

not contain the name of the patient of which the health information is about. The problem here is

that entities covered under HIPAA can provide third parties with this de-identified health data for

research or business purposes, but then that data is no longer protected under HIPAA, and is only

protected under whatever mechanisms of protection that the third party utilizes (McGraw et al.

2009). Another crucial aspect of this transfer of de-identified personal information is the ease at

which that data can be re-identified (McGraw et al. 2009). This is troubling because now

whenever medical records are wanted for medical research, it doesn't matter whether the data is

identifiable because in some way or another, that data can/will be identified and used for any

purpose by the third party that is not governed by HIPAA (McGraw et al. 2009).

The Privacy Rule enacted by HIPAA "imposes a minimum, uniform set of privacy

protections on public and private health care providers, health care organizations, and

others" (Slutsman et al. 2005: 832). The Privacy Rule also provides patients with access to their

medical records and gives patients the right to request a copy of their personal medical record

(McGraw et al. 2009). However, this right to access has not been implemented well at all, as failure to provide patients with their medical records upon request is one of the top five complaints about HIPAA to The United States Department of Health and Human Services (HHS) (McGraw et al. 2009). Since 1996, the rules regarding the penalties for noncompliance with HIPAA have never been enforced, and as of November 2008, HHS has not penalized a single HIPAA covered entity regardless of the fact that there have been multiple known violations (McGraw et al. 2009). McGraw et al. (2009) portrayed how HIPAA's Privacy Rule needs to be altered and extended in order for it to cover personal health information, and even then would it not be able to adequately protect the privacy of that health data.

In accordance with McGraw et al., Richard Sobel (2007) discussed how the HIPAA Privacy Rule's protection of private medical information is not what it seems to be. HIPAA is more of a disclosure regulation than it is a privacy rule and has undermined medical ethics by permitting the exchange of patient's medical information with such ease (Sobel 2007). The way patients perceive their privacy protection is usually determined by the initial encounter at whatever health institution they go to. Upon the arrival at said institution, many forms are filled out, including those forms involving notices of privacy practices and consent forms, which are easily misinterpreted as the same form when they are in fact different (Sobel 2007). The notice of privacy practices form usually contains such complex language that patients tend to misread the document and think that it is a consent form because like notices of privacy practices, consent forms are also written in general vague ways (Sobel 2007; McGraw et al. 2009). These forms are written by those entities seeking the health data, which is why they word the forms in a way that promotes misunderstanding and subsequent mindless signing of the forms.

The lack of control of personal information due to HIPAA may lead patients to avoid telling their providers important aspects of their medical history. Suspicions about the lack of confidentiality in the handling of personal health information have been known to discourage patients from sharing all of their information with their providers (Sobel 2007). A 1999 study showed that one in seven patients was actively keeping information from their providers by mechanisms involving going to different providers, paying out of pocket, and more (Sobel 2007). Once patients understand HIPAA and realize that under its regulations they have no say in who controls their health information, more patients will begin to withhold medical information from their providers. If the proportion of patients who do so gets large, physicians will need to start diagnosing patients without knowing the full extent of their patient's histories, which has the great potential of resulting in medical error (Sobel 2007). Studies have shown that although physicians have negative views towards HIPAA's Privacy Rule, they rate medical institutions with more Privacy Rule requirements better at protecting patient information than institutions with less Privacy Rule requirements (Slutsman et al. 2005). Evidence also suggest that providers see the Privacy Rule and rules alike as regulatory forces that limit their autonomy, and with the limitation of autonomy comes professional dissatisfaction and decreased quality of care (Slutsman et al. 2005). Physicians worry that the Privacy Rule not only lessens the protection of personal health data, but also hinders medical research (Slutsman et al. 2005; Annas 2003).

According to HIPAA, patient medical records can be used for research without the authorization of the patient if (1) the records are deidentified, (2) the records are a part of a limited data set where the data are stripped of most of their identifiers, or (3) an institutional review board (IRB) allows a waiver of consent under specific rules (Annas 2003; Damschroder

et al. 2007). All three of those components are flawed as deidentified data can easily be reidentified (McGraw at al. 2009), limited data sets still have identifying information, and the rules of an IRB can be vague in terms of privacy protection. This is why there have been such negative reactions to HIPAA's regulations in terms of the use of medical records in research, and it doesn't help that there are no national standards for providing researchers with confidential medical records (Annas 2003). In order for a change to occur in the realm of research, policymakers need to be doing a better job in explaining to patients why research is important, how it can impact their families and their health, and why the need for medical records is essential (Kass et al. 2003).

In 2009, the Health Information Technology for Economic and Clinical Health Act (HITECH) was signed into law to promote the adoption and meaningful use of health information technology (Blumenthal and Tavenner 2010). HITECH established incentive payments to providers when they utilize their EMR systems privately and securely, achieving specific improvements in quality of health care (Blumenthal and Tavenner 2010). The rule regarding meaningful use is part of a set of regulations to ensure the privatization and security of the EMR, and strikes a balance between realizing the importance of health information technology in the improvement of health care, and realizing the difficulties that come along with this implementation (Blumenthal and Tavenner 2010). The meaningful use objectives can be as simple as recording patient demographics, vital signs, medication lists and orders, diagnoses, smoking status, but can be as difficult as "implement[ing] systems to protect privacy and security of patient data in the [EMR]" (Blumenthal and Tavenner 2010: 502).

In a 2006 national survey, over 75% of the respondents were worried about the confidentiality of their personal health information, and over 50% were concerned about people other than their providers seeing their information. In order to establish public trust in health information technology there must be an implementation of more transparent and understandable public policies, better understanding of technological design, updated business practices, and efforts in patient education (McGraw et al. 2009).

Conclusion

Privacy, confidentiality, and trust are concepts that have been given a new sense of importance now that technology has given rise to the concept of electronic medical records. Privacy refers to an individual's ability to control the accessibility to his or her medical records; however, the literature is less clear about what kind of control patients desire (Cantor 2006). Moreover, the literature shows that patients tend to have more interpersonal trust than institutional trust, which may be in part due to the technological growth of this era (Mechanic 1998). When not worried about a lack of privacy in the system, patients were found to give more accurate information, and more accurate information can lead to more effective treatment and better patient outcomes (Sankar et al. 2003). However, patients definitions of medical record privacy and privacy amongst the medical staff is varied.

In order to understand how patients perceive their privacy in contemporary health care settings, we need to understand how patients perceive the use of and privacy of EMR, how patients understand and define the concept of privacy, and how and/or if patients feel that the implementations of EMR affects interpersonal trust, institutional trust, and privacy in general.

Chapter 2

Methods

The focus of this study was to determine how patients from two different health care settings perceive their privacy, and the role that electronic medical records play in the formation of those perceptions.

Sample

In order to address this topic, we conducted 44 in-depth, semi-structured interviews with a non-probability convenience sample of patients from one academic health care center (n=22) and from one federal hospital (n=22), both in the northeastern region of the United States. In order to protect the identities of the subjects interviewed, the subjects will be referred to by pseudonyms created for them. Each patient will be referred to as Patient 1, Patient 2, Patient 3, and so forth until Patient 44; this naming system will be used throughout the rest of this paper.

Study Support

I did not participate in the creating or the conducting of these interviews. Data were collected as part of a larger study on health information technology and privacy. This study was supported through federal grants from the National Science Foundation (NSF-CNS-0910842) and through the United States Deportment of Health and Human Services Office of the National Coordinator for Health Information Technology (HHS 90TR0003/01). Neither of the funding agencies had any role in the study design, management, analysis, interpretation, or approval of this study. This writing and the conclusions which I draw do not represent the views of the NSF

or the HHS. This thesis presents the primary analysis of only a portion of the interview data

collected through this grant-supported project.

Recruitment and Informed Consent

The research team that conducted the interviews posted advertisements throughout

hospital waiting rooms in order to recruit patient participants. The decision to participate in this

study was voluntary, the participation was confidential, and the participants were compensated.

Once a participant agreed to participate in the study, he or she was given an information sheet

that outlined participant rights and details about the study. It was only after the viewing of that

information and giving a subsequent verbal informed consent that the participants were able to

be interviewed. Neither names nor any other identifying information was gathered from the

participants. The interviews lasted from about 45 minutes to one hour using a semi-structured

questionnaire. Each interview was digitally recorded and conducted at the medical center

through which the participants were recruited. This study received expedited review and

approval from the Committee for the Protection of Human Subjects at Dartmouth College

(#22259).

Interviews and Data Analysis

The research teams at each hospital were tasked with conducting the patient interviews.

The interview started with asking general questions about the interviewee, including questions

about his or her health in general and a question to inquire the overall rating of the interviewee's

health care in the past year. The interviewers then asked about the interviewee's knowledge of

medical records in general, and continued by asking questions about electronic medical records specifically, assessing the patient's perceptions of the benefits and problems associated with EMR.

The last section of the interview focused primarily on privacy issues that may arise in the realm of the EMR implementation, and the interview concluded with a couple of questions regarding the Patient Portal. Throughout the interview, it was important for the interviewer to ask for specific examples from the interviewees in order to fully understand their responses.

Each interview was digitally voice recorded, transcribed, and analyzed using a qualitative analysis software program called Atlas.ti for Windows. The analyses of the data focused on understanding patient's perceptions of privacy in the health care setting, and the role that the EMR played in the development of those perceptions.

Questions, responses, and themes derived from those responses centered around how patients perceive: the major benefits and problems associated with EMR, how EMR affects doctor-patient relationships and the expectation of privacy and trust in those relationships, the importance of privacy and confidentiality of their medical information, the meaning of privacy in relation to medical records specifically and the differences in privacy between paper and electronic records, who is responsible for maintaining said privacy, and how much control the patient has in the protection of his or her information.

Chapter 3

Patient Perceptions of Electronic Medical Records

In this section of Chapter 3, I discuss the findings of the patient interviews conducted at two hospitals in the northeastern region of the United States. These data have much relevance to today's health care settings because most institutions have begun adopting the EMR systems into their everyday practices. As discussed in Chapter 1, there are many factors that come into play when a patient thinks about his or her medical record privacy protection, which can lead to issues within the doctor-patient relationship and a potential distrust in the physician or in the overall health care system. This portion of Chapter 3 will involve discussing the findings in the patient interviews regarding their views on the EMR, and how, if at all, they think that the transition from paper to electronic medical records plays a role in the relationships with their physicians.

Benefits of EMR

Most of the patients interviewed reported similar benefits that they see in the EMR system. The largest trend seen in the benefits of the EMR was the fact that it increases access to the records. In fact, 23 out of the 45 patients claimed that this increase in access was the main benefit of the new technology. Patient 17 reported that it is important for records to be accessible "between different aspects of the institution, different doctors even." Some patients made claims about the immediateness or instantaneous nature of the accessibly of the information stored in the EMR in that if you are traveling from your home to a foreign country and something happens in that foreign country, the records are able to be transferred there with ease. Patient 40 remarked, "…if I'm in California, they can send my records to California," noting the ease of

accessibility; whereas with paper, it would take a considerable amount of time to send the stack

of paper records via mail to California if the patient's records are sitting in a file cabinet in

somewhere like New York.

The speed at which the records can be sent somewhere was also a major benefit of the

EMR seen by patients. When discussing the accessibly of the EMR, Patient 10 also mentioned

how with paper records comes the delay of the dissemination of information. The speed at which

medical information can be shared was seen as a benefit by many, but also the speed at which the

information can be recorded. Patient 18 mentioned how a benefit of the electronic record is that

information can be typed faster into the system than it could be written by hand on a paper

record. Poor handwriting and the subsequent misinterpretation of information on paper were also

major concerns by many patients, which seemed to be why almost 50% of the patients claimed

that benefits of the EMR included increases in organization, efficiency, and accuracy of

information recorded in the system.

In terms of accuracy and organization, many patients noted that the handwriting of their

physicians has never been their strong suit, and in some cases has even led to misinterpretations

of written prescriptions or misinterpretation of a physicians note due to its illegibility. Typing

into the computer as opposed to writing on paper was seen as an overall benefit of the EMR as it

increases accuracy of information dissemination, but apart from the physical handwriting aspect,

the increased organization and efficiency that result from the EMR were also found to be

important to the patients. Patient 3 addressed the organizational benefit very simply: "The more

medically complicated you are, the more difficult keeping track of your care is." When paper

records were utilized, the more medically complicated you were, the thicker the stack of papers

became. In this manner, Patient 13 remarked, "…I like that [my doctor] has the medical record there because if we have to refer back to something we can. We don't have to dig though file and dig through a hundred pages." This saves time when the patient is with the physician and adds to the benefit of the fast nature of the EMR; fast, as in the speed at which the information can be obtained during the visit. This speed is directly correlated with the other benefit surrounding EMR which is that of efficiency.

Efficiency can be interpreted in many different ways, which is why the interviewed patients had varied discussions on the benefit of efficiency. Some patients like Patient 7 claimed that the efficiency of the EMR stems from the fact that the physician has the potential to accomplish "things" quicker, meaning the visit would be beneficially shorter and no one's time would be wasted. Patient 12 talked about the benefit of filling out online forms when going to the doctor's office as opposed to the clipboard of papers that are generally given to the patients upon arrival, stating it is "a more efficient way to give medical information." Patient 15 discussed the efficiency of EMR in terms of the physician being able to enter information into the system using templates, making that entering of information more efficient than writing a general note on a paper record. In terms of the template aspect of efficiency, Patient 39 commented about the ease at which information can be seen by using "key words" to locate specific information, which parallels Patient 13's remark about the organizational benefits of EMR. Patient 20 claimed that the EMR's beneficial aspect of efficiency could be taken to the level of the speed at which a prescription could be emailed to a pharmacy, which leads to less waiting and wasting of time.

Apart from accuracy, organization, and efficiency, another major benefit of EMR reported by patients was the increase in coordination of care. Patient 1 discussed the coordination aspect

in terms of a direct experience: "I have seen my internist in the morning and then gone to the hospital in the afternoon and the report she typed in is there already and blood test results are there." Like Patient 1, Patient 6 remarked, "I'm impressed that I can go and have a blood test done and then the lab work is sent electronically to the physician and she'll have it almost instantaneously…," portraying the coordination of care between the lab and the physician. Patient 2 discussed how the increased coordination of care is beneficial especially when transitioning between physicians; for example, when a patient goes to see a doctor for the first time, the patient's medical information is right there in front of the physician. Like Patient 2, Patient 30 and Patient 39 remarked, respectively, that the benefits of the coordination of care are that various doctors can have access, and the coordination aids in the "seamless transition" of information when consulting with more than one physician.

Some patients discussed the secure nature of the EMR as a benefit in comparison to the nature of the security of paper records. Patient 12 remarked how paper can get lost, whereas electronic records are backed up. Patient 21 claimed that paper is more vulnerable to fire, water, loss, being torn, and getting old, and how electronic records do not have the same vulnerabilities. In accordance with Patient 21, Patient 44 discussed the difficulties associated with EMR's being destroyed as they are most likely saved and backed up in multiple places, and that fire is a major vulnerability to the security of paper records. Patient 37 claimed to be inherently confident in the security of the EMR.

Another benefit of the EMR discussed by the patients was the environmental benefit of the use of computers as opposed to paper, which results in the reduction of hospital costs that can then be allocated to other areas in need. Patient 26 even noted that less paper equals less waste.

Only one patient, Patient 28, remarked that a benefit of the EMR was an increase in patient autonomy due to the transparent nature of the online records and the ability to "…see what the doctors said about me, [and] see my condition for myself." Another patient who stood alone in his or her remark, Patient 8, commented about the organizational benefits of the EMR claiming that EMR makes it easier to find habits and trends for research purposes because of how the data is organized in the system.

The major themes surrounding the benefits of the EMR discussed by the patients interviewed included: accessibility of the medical information, speed at handling the system, efficiency, organization, and accuracy of inputted information, coordination of care across institutions and medical professionals, security of the system, and environmental benefits. A few patients remarked that the pros of the EMR implementation outweighed the cons of the process; however, many patients were able to identify serious problems they anticipated facing during the implementation of this online system.

Problems with EMR

The patients interviewed were able to come up with many problems associated with the implementation of the EMR. The main issues discussed included: being error-prone, lack of user competence, time management, and the largest issues of them all, security issues.

In terms of being error-prone, Patient 1 discussed how he or she was waiting for test results that were taken in Florida to be sent to the hospital where he or she was being treated. The test results never ended up being delivered, so Patient 1 found a flaw in the EMR system to be that it is prone to "glitches." Both Patient 9 and Patient 14 respectfully noted that if the online

system shuts down for whatever reason, "…then everything comes to a halt," and the hospitals and physicians are just "tough out of luck." Like the concern that Patients 9 and 14 had about the whole system shutting down, Patient 22 worried about the EMR computer battery dying and the potential of lost information. Patient 15 was concerned about the EMR being error-prone because of its template layout and the ease at which a box can be incorrectly checked or something can be selected improperly.

In terms of user competence, only two patients had major concerns. Patient 6 expressed worry in regards to "…the competence of the [medical personnel] and their being up to speed as to how to use the system…," and Patient 31 remarked that the EMR technology was "…only as good as the person who's using it." Patient 31 left his or her elder physician who was having trouble opening a CT scan on the EMR for a younger, more technologically-adept physician as he or she found it extremely frightening that the older physician was unable to access such a scan.

Time-management was another anticipated problem according to a few patients. Patient 28 voiced a concern about the time it could take to locate information. Like Patient 6 and Patient 31's concerns regarding competence, Patient 28's time-management concern was similar. If a physician is unfamiliar with the EMR, he or she is more likely to take more time in order to find specific information in the patient file. The longer it takes to search for the information, the less meaningful time the patient has to spend with his or her physician, which Patient 28 viewed as a problem with the EMR. Patient 4 and Patient 11 also commented on the time-management problem with EMR claiming that it may take too long for information to be transcribed from a physician's note into the computer.

As important as the above concerns are in terms of the implementation of EMR, the concerns experienced by 86% of the patients interviewed (38 out of 44) were security concerns including: miscommunication, loss of information, hacking, and too much access.

The only patient who was worried about miscommunication was Patient 2, and the miscommunication referenced was in terms of an email. Email miscommunication between a patient and a doctor could lead the patient to do something that he or she should not be doing. Like a text message without proper punctuation, a misunderstood email can have a completely different meaning than its intended one. Apart from miscommunication, patients were also worried about the potential of losing information in the system if the records were not backed up properly, saved incorrectly, or hard disks crashing. Patient 21 expressed concern in this area by stating, "…computers can crash, back-ups can be lost." Patient 37 went as far as wondering where the information in the records is even stored.

The concern about hacking into the EMR system was expressed by almost a third (32%) of the patients interviewed. Patient 19 remarked that hacking was a worry because then the hacker would have access to medical information and personal information, like a social security number, which could even lead to, as Patient 43 puts it, "identity theft." In terms of the hacking concern, Patient 42 claims that, "whether there be problems, of course there will, but with technology moving as fast as it is, not only in computers but in life, you adapt to it and you move on. When you get holes in the wall, you patch the holes up." Patient 42 stands alone in the optimistic view point that the technological advancement of the EMR will eventually correct itself. Patient 9 and Patient 35 share the same point of view when it comes to hacking as a concern of the EMR. Patient 9 claimed, "I don't care who looks at my records. There's nothing

there I'm ashamed of… so I don't care if it's public knowledge," and Patient 35 claimed that he or she understood that hackers existed, "…but the fact is, who gives a damn if somebody hacks my medical records? Have fun… personally, I don't care." Both Patient 9 and Patient 35 portray an understanding of the concern, but a lack of considering it a viable one.

Under the umbrella of the too much access concerns lies the concerns about privacy, confidentiality, and inappropriate exposure. In terms of inappropriate exposure, Patient 38 gave a good example.

Well there's a huge black market use [of medical records] when you think about it. Employers would love to be able to get a hold of your medical records. And I'll be honest. If it was legal and I were in that situation, I would want to know what people's medical conditions were, because who wants to hire somebody who has a chronic illness and is just going to be out all the time… As an employer, I wouldn't want to hire a single mother or someone with a toddler, either, because you know, they've got other commitments and they're not always going to be the most beneficial to the company. (Patient 38)

In accordance with Patient 38, Patient 10 claimed that there is a potential for patients to be judged from the data in their EMR before the physician even meets the patients. Patient 10 continued and noted that a major problem with the EMR is that it provides access to those who the patient may not want to be looking at his or her records. Patient 44 agreed with Patient 10 in that Patient 44's mental health records were as accessible as the rest of the medical record and Patient 44 proclaimed that "there was no reason for the medical staff [at the hospital] to have known what I was discussing with my therapist." Patient 44 believed that mental health records

should be on a restricted portion of the EMR and should only be available on a need-to-know basis; Patient 44 believed it was a violation privacy and trust when various nurses were able to read the mental health information in the patient record. Patient 32 worried about unauthorized access into the system, and on the other end of the authorized spectrum, Patient 15 worried about those with legitimate access who may inappropriately divulge patient information. Patient 34 was also worried about too much access because Patient 34 went to buy life insurance, and the hospital that cared for Patient 34 gave the life insurance company all of Patient 34's medical records, which in turn, increased Patient 34's insurance rates.

In terms of privacy and confidentiality concerns with the EMR, Patient 14 explained that because the information is just out there, "exposed" on a screen, there is a greater risk of someone reading that information who should not be; Patient 14 claimed that that fact makes him or her "uncomfortable" and "questionable."

Now that the benefits and concerns associated with EMR according to the interviewed patients have been reported, the findings in regards to the effect that the EMR has on that relationship will now be discussed.

MAJOR *BENEFITS*	MAJOR *CONCERNS*
Increased accessibility	Security issues
Increased coordination of care	Too much access
Increased efficiency	Privacy/confidentiality concern
Increased speed at which information can be shared	Inappropriate exposure
Environmental effect	Hacking of the system
Increased security	Error-prone
Increased accuracy	Lack of user competence
Increased organization	Time management

Table 1. Outline of the major benefits and major concerns associated with EMR. The benefits and costs are listed in order such that the first benefit/cost listed was reported by the largest number of patients, and the last benefit/cost listed was reported by the smallest number of patients.

Effect of EMR on the Doctor-Patient Relationship

The effects of EMR on the doctor-patient relationship are important to study. Of the 39 patients who responded, 26% claimed that EMR had no effect on their doctor-patient relationship, 33% claimed that EMR had a negative effect on their doctor-patient relationship, and 41% claimed that EMR had a positive effect on their relationship.

Those who stated that EMR had no effect on the doctor-patient relationship did not list any reasons for their claims. That being said, those who claimed that EMR had a negative effect on their doctor-patient relationship discussed two major reasons. Ten of the thirteen patients who reported that EMR had a negative effect (77%) stated that the EMR made the physician seem non-attentive, and the other three patients (23%) stated that the EMR made the physician seem less personal. Patient 1 attributed the physician's non-attentiveness to the fact that when the patient was in the room, the physician claimed they were listening, but it did not seem that way to the patient: "…it makes me feel like a child again with a mother who is cooking and not paying attention to what I am saying…." Many other patients attributed the physician's non-attentiveness to the fact that he or she would simply stare at the computer screen while in a consult. Patient 17 claimed that his or her physicians "never even look at me when I go to see them." In reference to focusing more on the computer screen of the EMR rather than the patient, Patient 34 claimed that "…some [physicians] are more a slave to the machine than they are to the patient," which speaks volumes in terms of how some patients now perceive their physicians in this technological age. Patients 20 discussed how his or her physicians would stare at their computer screens, which Patient 20 attributed to having a negative effect on the overall doctor-patient relationship.

I've noticed that there are some doctors or nurses who, when they have the laptop in front

of them, that's what they're looking at. They're not looking at you, Thats kind of annoying

to be honest with you…I've had one or two [physicians] who are more engrossed with

what's on their screen than in their conversation with me. (Patient 20)

Patient 22's response paralleled that of Patient 20's in claiming how the doctor-patient

relationship is negatively impacted by the presence of the computer.

[The physician's] focus is more on the computer than directly with me…They don't look

at the file before they come and see me. They are looking at it while I'm there, [and I

think]… it's good that they can pull everything up, but at the same time they're not

focused directly on me now. They're focused on the computer screen. (Patient 22)

Both Patient 23 and Patient 28 believed that the distracting nature of typing on the EMR caused

the negative effect on the doctor-patient relationship, and Patient 23 explained this phenomenon

well: "The worst part about the whole electronic thing in a doctor's office is you are sitting

there in pain, or you are trying to explain what happened to you yesterday, and all you can hear is

click click click click click click click click." Patient 12 even remarked that some patients may

even be intimidated by the sheer presence of the laptop in the room.

Unlike the reason of general non-attentiveness, Patient 4 attributed the EMR's negative

effect on the doctor-patient relationship to the impersonal nature of the interaction that resulted

from the use of the EMR: "I think you actually interact with [the physician] less; less as a person,

I want to say more of a mechanic…a person who is just entering information…." Patient 16 even

stated that "…when they're asking you questions [while using the EMR], you don't get that

personal feeling, like they're [not] really interested in you," portraying the impersonal feeling experienced by patients due to the presence of the EMR.

Those who claimed that EMR had a positive effect on their doctor-patient relationship also discussed two major reasons. Eleven out of the sixteen patients who claimed that EMR had a positive effect (69%) stated that the EMR allows physicians to keep up with the changing medical knowledge in the general field and to keep up with the changing medical information of their patients. Patient 6 remarked that the laptop that houses the EMR is a "useful tool to help them help me," which correlates with the physicians ability to keep up with the patient's medical information in the EMR. Patient 39 claimed that the EMR had a positive effect on the relationship with his or her physicians because Patient 39 has a bad memory and benefitted by the EMR because it helped Patient 39 remember all parts of Patient 39's medical history. Many of the patients who responded in claiming that the EMR had a positive effect attributed this to the fact that EMR makes medical information more readily available, be it information about the specific patient, or information about a new technique/mechanism used to treat and cure patients.

The other five patients who claimed that EMR had a positive effect (31%), stated that the EMR facilitates the interaction between the physicians and the patients. Patients 3, 5, 12, 42, and 43 each discussed how the EMR improved the interaction between doctors and patients due to the EMR being able to free up the doctor's time; it takes longer to write than it does to type. Thus, the physician would be able to accomplish more in a shorter period of time, beneficially speeding up the interaction. Patient 40 was the only patient to claim that due to the lack of paper, the physician would be able to focus more on the patient, facilitating their interaction. Patient 32

even went as far as claiming that "…[the use of the EMR] helps me communicate better" with his or her physician.

Importance of Trust in the Doctor-Patient Relationship

When patients were asked if trust was an important part of the doctor-patient relationship, 56% of the 34 patients who responded reported trust being "very important" and 44% of the 34 patients who responded reported trust being simply "important." Patient 4 claimed that trust is very important because "…I just figure it's all going to reflect in positive care for me." In reference to the importance of full disclosure, Patient 7 remarked, "…if you don't have the trust, you are not going to tell them everything." Patient 18 claimed that trust was an important part of the doctor-patient relationship because "…you have to trust [the physician's] professional ability…," and Patient 20, who also felt that trust was an important aspect of the doctor-patient relationship, claimed, "… you need to feel you can trust [your physician] with any information that you give them, so that when something goes downhill, they can respond to it, and help you." Interestingly, Patient 33, who claimed that trust was a very important part of the relationship, said that "You never think of [the doctor-patient relationship] in terms of trust until it's violated."

Many of the patients who responded claimed that in order for the doctor to give the patients the care that they need, patients need to trust their doctors and trust that their doctor's advice and treatment plans are only in the best interests of their patients. Some of the patients who claimed trust was very important said that they trust whatever the doctor says, but did not specify why.

Patients were then asked a follow-up question regarding whether they considered the relationship with their doctors a trusting one, and why. Of the 36 responding patients, 83% claimed that they completely trusted their doctors, 14% claimed they had limited trust in their doctors, and only one respondent claimed to have no trust in his or her doctor. Those who stated that they only had limited trust in their doctors were Patient 14, Patient 16, and Patient 22. Patient 22 claimed to have only limited trust in his or her physician because of their relationship being not well-established: "… I have confidence in [my physician's] decisions and suggestions, just because they've been trained as a doctor, but I don't know them, and they don't know me as a person, or my situation, on a regular basis well enough to say that there's actual trust." Patient 16 had limited trust in his or her physician because he or she did not believe that the doctor really cared about the patient and was more focused on the clock, and Patient 14 had limited trust in his or her physician because he or she was worried about inappropriate exposure in a social setting: What if he "went out some night or whatever and started talking to other medical friends? Who knows? If he drinks a little bit too much, maybe he talked a little bit too much."

Of the 35 patients who stated that they trusted their physicians, seven major reasons for the establishment of that trust were reported: the professionalism of the physician (43%), institutional trust (37%), the amount of time spent with the physician (14%), the physician's personality (14%), and the fact that their physician listens to them (11%).

Those who claimed to trust their physicians because of their professionalism characterized their doctors using the following adjectives: knowledgable, intelligent, skillful, competent, caring, honest, and respectful. A few patients also defined the professionalism of their physicians to be their physician's ability to treat and cure illnesses, which can also be defined as

their skill. Patient 10 simply stated that the trust in his or her doctor stemmed from the fact that "…he knew what he was talking about… [and was] still receptive to amending [his] opinion and [his] decision and [his] judgement when [he's] given new information…." The largest percentage of respondents attributed the establishment of trust in the doctor-patient relationship to their physician's professionalism.

Those patients who stated that they trusted their doctor "because he/she is a doctor" or because they trusted their doctors "no matter what" were placed into the category of institutional trust because if you trust your doctor simply because he/she is a doctor, you are trusting the institution because it is the institution that chooses those doctors. The second largest percentage of respondents attributed the trust in their doctor to institutional trust.

The amount of time the physician spends with the patient, the personality of the physician, and the fact that the physician listens to the patient are the rest of the major reasons why patients reported trusting their physicians. In terms of personality, some patients gave no specific reason, and others simply claimed that they liked their physicians. Patient 38 claimed to have trust in the physician because of the physician's ability in "…remembering things from visit to visit or at least looking [them] up. Caring about the whole person, not just that particular ailment." Patient 20 remarked that, "there's nothing worse than feeling like you've been shuffled in and shuffled out of an office," which is why Patient 20 attributed trusting the doctor to when they listen to the patient and when they spend time with the patient.

Only one patient claimed that they trusted their physician because the patient's life is in the physician's hand, and only one patient claimed that they trusted their physician because "the physician is accountable for maintaining confidentiality in practice."

The only patient who claimed that he or she did not have any trust in his or her physician was due to the fact that he or she had not spent enough time with his or her physician, and therefore had not established a relationship: "I guess until I have some kind of a medical condition that's going to require me to have an interaction with [my physician] over a regular basis, then I would be able to develop a trust with her. Right now it doesn't exist."

Understanding how patients perceive EMR in terms of its costs and benefits is important in understanding how patients perceive the EMR affecting the doctor-patient relationship. The dynamic relationship between the patients and their providers that results from the implementation of EMR will certainly affect how patients perceive and understand the concept of trust within the doctor-patient relationship. This is why understanding how the EMR affects the doctor-patient relationships is crucial in forming an understanding of the patient perceived importance of trust within the doctor-patient relationship. Now that those concepts have been reported, patient perceptions of privacy including expectations and concerns of privacy, definitions of privacy, and the effect of EMR on patient privacy will be reported.

Patient Perceptions of Privacy

In this portion of Chapter 3, I report the findings in the patient interviews regarding the patient's definitions and expectations of privacy, and how EMR, if at all, effects how patients perceive their privacy.

Expectations and Concerns Regarding Privacy

When asked about their expectations and concerns regarding privacy within the doctor-patient relationship, 36 patients responded out of the 44 patients interviewed. 28% of patients believed that medical information can be shared amongst providers, but only with previous patient permission, 22% expected complete privacy, 17% expected to not be informally discussed, 17% had no concerns with any aspect of the privacy, three patients believed that medical information could be shared amongst providers without patient consent, two patients had low expectations of privacy, and one patient expected no privacy in terms of the protection of their medical records.

Patient 7 expected that medical information should only be shared when the patient has given permission and recounted an interaction: "'Is it okay if I share?' [My doctors] always say that. I really like that…" Patient 12 had the same expectation at Patient 7 and wondered, "If you go to the foot doctor, should he be able to access every moment you had with any doctor?" Like Patients 7 and 12, Patient 22 expected the sharing of information to be only between those who the patient had previously permitted, and commented that nurses should not be able to access the whole medical record, but only portions of it. Patient 30 shared the same expectations, but presumed that any sharing of information between medical personnel should be anonymous unless that medical personnel was directly caring for the patient. Three of the responding patients also expected that information would be shared amongst their providers, but did not expect their permission to be necessary. Patient 4 remarked that more collaboration between providers leads to more knowledge, and Patient 15 expected "a general, reasonable amount of confidentiality, but openness when it's necessary…."

Patient 19 was part of the 22% of patients who expected complete privacy of their medical records. Patient 19 expected that everything should be private unless the information became legally necessary. Patient 26 was also part of that 22% and expected the same privacy as would exist when telling a close friend something important and secretive. Most of the patients who responded by expecting complete privacy and confidentiality did not give specific examples as to their definition of complete, but simply expected it.

17% of the responding patients expected their physicians to protect their patient's privacies by not informally discussing their patient's medical information. Patient 1 said, "I suppose that I wouldn't be gossiped about in some kind of trivial way…" Patient 9 discussed how the privacy of patient medical records has the potential to be violated if it were to be discussed in an improper setting, somewhere other than a health care facility: "No one likes being made fun of. I wouldn't care to know after the fact that whatever condition I might have had was being made light of at someone's dinner party for instance." Similarly, Patient 13 claimed, "It would be nice if [physicians] weren't discussing you over their dinner table," but was also okay with being anonymously referred to for collaboration purposes.

Six of the thirty-six responding patients had no concerns with how privacy is handled. Patient 11 had no concerns because he or she had nothing to hide in his or her record. Two of the thirty-six responding patients had low expectations of privacy. Patient 10 had an encounter with a physician who knew something about Patient 10 before Patient 10 had the opportunity to mention it. Patient 10's low expectation of privacy protection stemmed from "…the fact that this doctor came up to me and said why is this information not in there? Well, he knew it and I hadn't told him." Patient 38's low expectation of privacy was due to the fact that medical personnel

used last names when referring to patients within earshot of other patients in the hospital in which Patient 38 was receiving care. Patient 2 was the only patient expected no privacy because he or she had no faith in the system, "I pretty much have assumed all my medical records are out there now [for everyone to see]…."

The previous portion of this section addressed the expectations and concerns regarding privacy within the doctor-patient relationship, but this portion will address patient's privacy concerns when medical personnel interact with each other.

Of the 40 patients who responded to this question, 80% had no concerns. Patient 2 had no concerns about privacy because he or she was more concerned with his or her health. Many of the 80% of patients who expressed no privacy concerns were confident that any interaction between medical personnel would only benefit patient care. Patient 4 claimed that any interaction between medical personnel would be a "positive collaboration," Patient 26 would rather "have more opinions than one," Patient 28 claimed that the interaction would only consist of "talking about my health for my benefit," and Patient 42 claimed that the interaction "would be an advantage because no individual knows everything, so to share information with somebody else… is a good thing."

The 20% of responding patients who did have concerns with their privacy when medical personnel interact were worried about being informally or inappropriately discussed. Patient 12 claimed that patient information should only be discussed between providers if the patient had previously permitted the disclosure of his or her personal information. Patient 15 was concerned with the fact that sometimes medical personnel discuss the personal information of a patient within earshot of other patients, or as Patient 23 and Patient 25 described, discussing personal

patient information public. These patients believed that those discussions were better held behind closed doors. Patient 10's attitude towards this privacy concern was concisely stated: "…it's all about the balance between privacy and providing good care."

This next portion of this section will address the findings when patients were asked their personal privacy concerns. Of the 36 patients who responded to this question, 75% of them had no concerns with their own privacy. Patient 1 reported feeling unconcerned about his or her personal privacy because he or she simply wanted the best care possible. Patient 28 was unconcerned because he or she felt that "…[his or her privacy] is well, well guarded." Patient 22 was also unconcerned, but unlike Patient 28, Patient 22 believed that …[his or her privacy] is at risk when [medical personnel] leave computers unattended…"

The remaining 25% of responding patients were concerned with their personal privacy for a few reasons. Six patients were concerned with the locations in which medical personnel discussed specific patient information and believed this was done in too public of places and instead should be done behind closed doors. One patient was concerned with the potential inappropriate sharing of personal information without patient consent, and another patient was concerned with his or her privacy when it reached the insurance company, claiming that insurance companies can use personal medical information to potentially raise deductibles or premiums and profit financially. Patient 10 reported an interesting concern regarding unnecessary personnel working on a patient because he or she was an interesting case: "Doctors [were coming] into my hospital room because they were curious. I'm sorry, that's offensive. I'm not a zoo exhibit. Go away. If you have no reason for being here, like aside from that's kind of fascinating, that's not treating me with regard."

Definition of Privacy in Relation to EMR

Of the patients interviewed, 28 of the 44 patients responded the the question that asked them to define privacy in relation to medical records specifically. 64% of the patients who responded defined privacy in terms of who has access to the medical record, 18% of the patients who responded defined privacy in terms of the security of the sensitive information in the medical record, 14% of the patients who responded had not put much thought into it and could not come up with a definition, and one patient defined privacy in relation to having a secure system in which the medical records are stored.

Patient 43 was the only patient to define privacy in terms of the security of the system; Patient 43 claimed that there was a need for "a very secure server," and stated that, "you should have a password to get on a web site, you should have to have a password to view files. It should be encrypted." The 14% that responded by saying they had not thought about the definition of privacy did not state anything else in terms of this question. That being said, those who defined privacy in terms of the security of the sensitive information in the medical record had more to report.

In terms of defining privacy relative to how sensitive information is stored in the medical record, Patient 5 reports: "…I can certainly understand [how] people with some kind… of contagious diseases or transmittable diseases would be very, very concerned, and I can see where they might be unwilling to have their records electronically recorded." Patient 21 and Patient 26 each claimed that in order to maintain privacy of medical records, personal information and more serious illnesses like sexually-transmitted diseases should be kept confidential. In accordance

with Patients 21 and 26, Patient 20 defined privacy in terms of the inability of sensitive

information in the EMR to be easily traced or de-identified.

> What I'm hoping though is that [serious information is] going to be detached, like not
>
> traceable to my [general] history. That's what I would expect. The information is there,
>
> but just a number on a page, or it's just part of pie chart… and completely separate from
>
> my actual health history. (Patient 20)

Aside from defining privacy in terms of how sensitive information is kept private, most patients

defined privacy in terms of who has access to the medical records.

Of the 18 patients who defined privacy in terms of access, 2 patients defined privacy in

terms of the medical records only being shared within the health care institution, 4 patients

defined privacy in terms of who has general access to the records, 5 patients defined privacy in

terms of the medical records being shared with only those who the patient has permitted, and 7

patients defined privacy in terms of the fact that there is the potential for too much access within

the EMR system.

Patient 5 was one of the patients who believed that privacy should be defined in terms of

the fact that there is the potential for too much access within the EMR system, and claimed, "I do

think that having EMR… does open a bunch of doors to letting other people know what's going

on." Patient 7 clarified Patient 5's claim in that Patient 7 stated that medical records should not

be left in a vulnerable position where they can be accessed without authorization. Patients 23, 29,

and 38 all stated that the medical records should be "locked tightly" in order to restrict access

from those who may be attempting to gain it. Patient 39's response to this question of privacy

directly correlated with those patients who believed that EMR has the potential for too much

access: "There should be protocols in place so that access to the medical records are restricted to linked personnel, so that if there's a doctor… [that is attempting to gain access, but] has no reason to look at my medical records, that doctor should not be allowed to look into them." Patient 41 breaks the definition down into even more specifics, "…if you're an MD, then you can access anything in the record. If you're a nurse, you can go about so far. If you're the janitor, you can't turn the machine on."

The other way in which patients defined privacy was in terms of the fact that the only people who should have access to the medical record information are those who the patient has permitted. As Patient 11 claimed, the physician is "… not allowed to disclose [patient] information without the patient's permission…," and Patient 40 claimed that privacy meant "you don't share [my information] with other people without my permission." In a similar fashion, Patient 24 remarked: "Everybody that's treating you needs to have access to your medical record…," expressing the fact that the entire medical team on the patient's care should have access to the patient's record. Patient 42 claimed that his or her medical records should only be able to be accessed on a "need-to-know basis," paralleling the other claims about access only when the patient permits it. Lastly, Patient 19 articulated his or her privacy definition in terms of the fact that the only people who should have access to the medical record information are those who the patient has previously permitted: "… I think you should be able to have total control over your records and your patient medical history and just be able to release it to the people that you want to see it."

Effect of EMR on Patient Privacy

Patients were asked how EMR affects patient privacy differently than paper records. Of the 35 responding patients, 69% claimed EMR makes access easier thereby decreasing patient privacy, 17% claimed privacy was affected no differently with EMR than with paper records, 11% claimed EMR makes access harder thereby increasing patient privacy, and one patient discussed the difference in terms of the physical nature of the two methods of record storage.

The majority of patients who responded reported that EMR was easier to access than paper records, decreasing patient privacy. Patient 2 and Patient 5 both discussed how the EMR was easier to access because of the possibility of medical personnel leaving the EMR screen open inappropriately for other, potentially unauthorized, personnel to view. Patient 9 also claimed EMR to be more easily accessible than paper and remarked that "…[someone] with a computer couldn't hack into a paper system." Patient 11 discussed the online nature of the EMR in being responsible for its increased access: "You [used to have to be] in that office to get [the paper records]. Now, you could be 100 miles away… and get into that system of electronic records." Patient 19 also thought that EMR was more easily accessible than paper records, but only slightly more, stating: "You can still make a copy of a paper file or check out the paper file and show it to somebody else," showing a vulnerability of the paper records as well. Patient 35 agreed that the EMR was more accessible, but did not think that it affects the patient's privacy in any way: "…I don't think it affects the patient because, what are they going to do with [the record]? At the end of the day, my medical record is not going to… indict me in any way, shape, or form that is of any consequence to what I consider to be my normal life." Patient 44 attributed the EMR in decreasing patient privacy in relation to mental health.

[In the EMR], it was all right there and the mental health records were mixed in with my

medical records… I feel that the paper record would have provided more privacy simply

because [the doctors] would have had to make a special effort to go up to the [psychiatric

department] and request my record and take my record out to read it. (Patient 44).

The 17% of patients who claimed that privacy was affected no differently by EMR than by paper

records did not give any specific examples that backed their claims, but Patient 38 did remark

that both paper records and EMR have their own vulnerabilities.

11% of patients claimed that EMR was harder to access than paper records, thereby

increasing patient privacy. Patient 13 commented on the vulnerability of the paper record versus

that of the electronic record: "The [patient] chart is hanging outside a doctor's office all day long.

It's easy enough to walk by and grab that hunk of paper…, [but if the record was stored in a

laptop], nobody can see it. Nobody can access it. Nobody can read it." Patient 22 commented on

the security of the EMR versus that of the paper records in that it would be harder to access

EMR: "[On the EMR] you have to sign in with a password and stuff, which means the computer

can keep track of that, which is more secure than just a paper log."

Only one patient commented about the physical nature of the paper records and the EMR,

and stated that paper can be destroyed or misplaced, but information stored in the EMR "stays in

the computer."

Patients were asked a follow-up question to the question of how EMR effects patient

privacy differently than paper records that asked whether it was more or less likely that patient

records could be exposed now that they are electronic as opposed to on paper. Of the 29

responding patients, 62% reported that exposure was more likely, 28% reported that exposure

was less likely, and the remaining 10% reported that exposure was equally likely whether information was stored on paper or within the EMR.

Patient 1 reported information exposure to be more likely in EMR because of the security issues surrounding having a password to access the EMR: "Anybody who has got the password to the medical records system [could do anything]." Patient 3 attributed the increased likelihood of exposure to its online nature: "Anything that's online is open to hacking and anything that's open to hacking can be exposed." Patient 16 was concerned with the technological era in general, stating, "I think the electronic world has created a huge situation where the potential for breach of privacy is just tremendous." Patient 31 also believed information exposure was more likely by using EMR but claimed to have "confidence in the system" in that his or her privacy would be safe. Patient 39 commented on the physical nature of the paper records in that it makes them more secure than the online records stored in the EMR. Patients 41, 42, and 43 all attributed the increased likelihood of information exposure by using the EMR to the existence of hackers, who have the potential to break into the system and steal personal health information.

The 10% of patients who reported that there was no difference in the likelihood of exposure of patient information did not report any particular reasons why; however, the 28% of patients who reported patient records were less likely to be exposed by using EMR, thereby increasing patient privacy, did state specific reasons. Patient 13 claimed EMR to be less likely in exposing patient information because "there's no access to [the EMR]. There's nothing hanging outside the door saying that that's who's here." Some patients reported exposure to be less likely because of the password protections and encryptions that come along with the online nature of the EMR; Patient 37 claimed that "there's too many safeguards that are in place." Patient 26

attributed EMR in being less likely to expose patient information, thereby increasing patient

privacy because of the physical nature of the different record systems: "Paper, what happens if

there's a fire? Where is the info? If your computer crashes, you might lose it too, but I'm sure

there's a backup somewhere."

Responsibility and Control of EMR

In this portion of Chapter 3, I report the findings from the patient interviews regarding

who or what entity is most responsible for ensuring the privacy of patient health information and

why, and if that person or entity is capable and committed in protecting that privacy. This portion

will also report how much control patients believe they have in protecting the privacy of their

records and if that control should increase, decrease, or not change at all.

Entity most responsible for ensuring the privacy of EMR

Of the 41 patients who responded to this question, 35% of patients claimed that the

hospital and its administration were responsible for the maintenance of the privacy of EMR, 33%

of patients claimed that those who worked in the medical records department were most

responsible, 13% claimed that the physicians were most responsible, 9% claimed that the

patients were most responsible, another 9% claimed that everybody who has access to the record

was most responsible, and one patient claimed that the insurance company was most responsible.

Patient 3 was of the 35% of patients who claimed that the hospital was most responsible

for ensuring the privacy of medical records and reported this way because Patient 3 believed the

hospital to be the entity that physically maintained the records. Patient 17 reported in the same

way as Patient 3, and claimed that the hospitals are the ones "that are sort of getting all the

information together and keeping it in one unit…" Patient 18 attributed the responsibility of the

maintenance of EMR privacy to the administrators of the hospital because they are the ones who

"set the policy," and Patient 19's response paralleled that of Patient 18's when he or she stated

that the administration has "control over the electronic system that holds the files." Patient 26

also reported the hospital and its administration to be the entity most responsible for ensuring

privacy of medical records and claimed that the hospital and its administration are "the ones that

have taken the information. They're the ones that should keep it and store it. Anybody needs to

access [the EMR] should be able to…" Patient 43 shared a similar opinion to that of Patient 26

and reported the hospital administration is most repressible because they are "responsible for the

actions and inactions of everybody on the staff."

The second largest percentage of patients (33%) believed that the responsibility of

ensuring privacy of medical records rested in the hands of those who worked in the medical

records department. Patients who responded this way reported these medical record deportment

people to either be information technology (IT) experts or people in a physical department of a

hospital that safeguard the servers or main database of the EMR. Patient 8 claimed that "whoever

is in physical custody of the [EMR] is responsible for securing it." Patient 13's claim

complemented that of Patient 8's and stated that the people in the medical records department

"should be like the CIA of the hospital. Nothing gets in and nothing gets out…" Similarly,

Patient 44 attributed the most responsibility to those working the medical records department

because they are the ones who set the EMR up in a "certain way with firewalls or passwords or

safeguards or what have you so that access would be restricted only to the people who need-to-

know…" Patient 33 attributed the responsibility of privacy protection to the fact that those who work in that department "have access to the accumulation of that information," and as Patient 27 commented, "if somebody is snoopy, like somebody that works in the [medical records department], and they see the name of one of their neighbors and she's had an abortion or something and they go blabbing… that could cause a lot of problems." Patient 32 interestingly reported that the medical records department was most responsible for ensuring privacy of the EMR because "they're the ones that are supposed to be checking for all the leaks and how to go about fixing them."

13% of the responding patients reported the physician to be the most responsible entity in protecting the privacy of the information in the EMR. Patient 2 reported this way because the doctor is "the first person you go to when something is wrong." Patient 40 also reported in this manner and thought that the doctor was most responsible for ensuring privacy of the EMR because "[the doctor] probably [has] the password to get to my medical stuff."

9% of the responding patients reported the patient to be the most responsible entity in protecting the privacy of the information in the EMR, and Patient 10 reported in this way because he or she felt that "nobody cares about your issues like you." Patient 12 also believed the patient to be the most responsible entity in protecting privacy of EMR because the patient has control over what goes into the EMR: "I think the patient should just say if [he or she doesn't] want [something] to be electronically recorded… [The patient gets] to decide what information gets disseminated around the world." Patient 23 claimed that because it is the patient's personal information, it is their job to check up on it, and stated: "You know, I may not know how to fix my car, but it's my responsibility to make sure that it gets into the shop every once in a while."

The 9% of patients who reported that everybody who had access to the EMR was responsible in ensuring privacy in the EMR did not give specific reasons or examples to back up their claims and simply stated that because the medical personnel has access, they should therefore be responsible for the information that they are accessing. Patient 2 was the only patient who related the idea of responsibility to the insurance companies and claimed that because those companies have access to all medical information, protecting the privacy of that information was "the least they could do."

Entity most responsible for ensuring/protecting privacy
Hospital Administration
Medical Records Department
Physicians
Patients
Anyone who has access to EMR
Insurance Company

Table 2. Outline of most responsible entities chosen by patients in ensuring/protecting privacy. The entities are listed in order such that Hospital Administration was chosen by the largest number of patients, and Insurance Company was chosen by the smallest number of patients.

Capability of that entity in protecting the privacy of EMR

Of the 37 patients who responded to the question of whether the entity identified as the most responsible for protecting the privacy of the EMR was capable of protecting that privacy, 81% reported the entity to be capable, 11% reported the entity to be incapable, and 8% were unsure.

Patient 4 reported that the hospital administration was capable in protecting the privacy of EMR, but only reported that way because of an inherent trust in the system, or an institutional trust. Patient 7 similarly reported the hospital administration in being capable of protecting privacy, but reported this way because he or she trusts them, and had "no reason not to." Patient 39 reported this way as well, and claimed to trust that the hospital administration was capable "because they have the appropriate mechanisms already in place, and they have access to security protocols that private organizations may not." Patient 22 also reported this way, mentioning the hospital's capability in securing the system. However, there were also patients, like Patient 43, who reported that the hospital administration was capable at privacy protection for the sole reason that his or her personal records "[haven't] been compromised."

Patients 11 and 15 deemed those who worked in the medical records department of the hospital capable of protecting the privacy of the EMR because they believed that they were "try[ing] really hard," whereas Patient 32 claimed that they were capable because "they're the guardians at the gate…," the gate referring to the first-line of defense against security breaches.

Patient 24 reported the physician capable of protecting the privacy of the EMR because "…they're trained for it. You know, they go in everyday to make sure everything's updated."

Of the 11% to report their entity of choice being incapable of protecting privacy, two patients reported the hospital to be incapable, and two patients reported the patient to be incapable. Patient 9 reported the hospital incapable of protecting the privacy of the EMR because of its flawed and seemingly irreparable security system by stating, "…if the Pentagon can be hacked, I certainly think that hospitals don't begin to have the security that the federal government does." Patient 41 reported in the same manner as Patient 9, but attributed the

hospital's lack of capability in protecting the privacy of EMR to its size, claiming the hospital is "…too large an elephant to feed. They need to have a team that will take care of [protecting the privacy of EMR] and I don't believe they do." Two patients (Patient 10 and Patient 23) reported the patient incapable, but also claimed that some patients may be capable.

Of the three patients who reported being unsure whether the entity of their choice was capable of protecting the privacy of the EMR, one patient was unsure about the capability of everybody who had access to the EMR, one patient was unsure about the capability of the physicians, and one patient was unsure about the capability of the hospital but still had trust in the institution.

Being capable of protecting the privacy of the EMR is important, but being committed to protecting that privacy can be considered even more important. Of the 41 patients who responded to this question, 59% reported their entity to be committed, 7% reported their entity to be uncommitted, 7% reported that the commitment of their entity depended on something else, an 27% reported feeling unsure, but optimistic that their entity would be committed.

Patient 15 reported that the medical records department was indeed committed to protecting the privacy of the EMR, and reported this way due to a feeling of institutional trust: "I trust that there are enough smart people with good intentions who are talking it through or doing this. Again, maybe it's somewhat misplaced faith in a system like that, but I prefer to feel that way, because I think it could be true." Patient 20 also believed the people of the medical records department to be committed and claimed, "I trust the integrity of the professionals… maybe it's just too trusting… [but] I trust they'd want to do their job well," portraying Patient 20's trust in the institution. The majority of those who chose the medical records department personnel as the

most responsible for ensuring the privacy of the EMR also reported them being capable and committed, but believed in their commitment because they reported it was their job to be committed; some patients did not have reasons for their claims. That being said, Patients 5, 27, 29, and 34 reported feeling unsure, but optimistic that those who work in the medical records department were committed to protecting the privacy of the EMR; Patient 1 was the only patient to report that the commitment of those people depended on the individual person.

Patient 44 was the only patient to report the medical records department personnel in being uncommitted in protecting the privacy of the EMR because the patient did not like the fact that you can see information regarding mental health information just as easy as information about a broken bone, claiming a patient's record is like "one big room. So you walk in the room and you see the whole room." Patient 44 reported a need for better "compartmentalizing" of the EMR.

Patient 18 reported the hospital committed to protecting privacy "for no other reason than to cover their ass," referencing the hospital's liability in privacy protection. Patient 22 also referenced the hospital's liability in considering the hospital to be committed to privacy protection, and also claimed that it was liability alone that made the hospital committed, "and not because they so much care [about the patient's privacy] on a personal level." Patient 35 reported the hospital to be committed because of the physical signs and notices around the hospital "telling not just the professionals to respect patient privacy, but telling other [hospital personnel] and other patients to respect the guy's privacy in front of you." Patient 35 also acknowledged the signs in the hospital, but reported feeling unsure, but optimistic in the commitment of the hospital to protecting privacy: "There are signs all over the hospital that say 'Please stand 20 feet

back' to prevent people from overhearing the kinds of exchanges that take place between an intake clerk and a patient. You don't have any conversations about your medical care in the waiting room." Patient 7 reported the hospital being committed, and posed an interesting question: "If [the hospital personnel] are not committed, then who would care what people think [about their commitment]?"

The patients who reported feeling unsure about the hospital's commitment to protecting the privacy of the EMR were generally optimistic in their uncertainty. Many of the patients who felt this way reported that they did not know about or simply hoped that the hospital would be committed. Patient 16 claimed, "If [the hospital is] committed to maintaining confidentiality, I would think that [the hospital] would have to be [committed] in order to maintain their integrity, [and] the trust of the public." Patient 41 was the only patient to report the hospital administration to be uncommitted in protecting privacy, and claimed this way because "…they have way too much work to do."

In terms of the physician's commitment in protecting the privacy of patient's medical information, Patient 37 attributed the physician's commitment to his or her professionalism claiming that the professionalism dictates the commitment. Of the three patients who reported being unsure about the physician's commitment, Patient 9 reported being unsure, but optimistic, Patient 10 reported that it depends on the individual physician, and Patient 2 claimed that "…it's very clear to me now, when I walk in [to a physician's office], whether the office is committed or not, just by the initial interaction," but did not report the specifics of what the initial interaction referred to.

In terms of the patient's commitment in protecting the privacy of their own medical information, Patient 23 and 25 claimed that, yes the patient was committed, but Patient 12 reported patients being uncommitted to protecting their own privacy and would only become committed if their privacy became implicated.

Patient 14 was one of the patients who reported that everybody who has access to the EMR in being most responsible for ensuring privacy of the EMR, and claimed to be unsure whether those people are capable in protecting that privacy, and unsure, but optimistic in their commitment thinking that commitment to privacy protection was part of their job: "I always thought that's the way it was. I don't know why. I just always thought that's the way it was," reflecting inherent, or institutional, trust in the system.

Patient control in protecting the privacy of EMR

Of the 43 patients who answered the question of how much control they had in protecting the information in their EMR, 65% reported having no control, 34% reported having some or minimal control, and one patient reported having no idea how much control he or she had. The responding patients were then asked a follow-up question regarding whether the patient felt as if he or she should have more control in the protection of their EMR.

Of the 65% of patients who claimed to have no control in the protection of their records, 61% of those patients reported that they should not have more control. Patient 3 claimed that having more control over your records was not possible and stated, "I'd love to be able to take stuff out… but putting stuff in…there's really not anything you can do about that." Patient 6 also felt this way and claimed, "…I think there's too much concern about privacy. I'm more

interested in getting the best possible care… [my medical records are] in the care of other people who I trust and I assume to be competent." Similarly, Patient 34 stated that he or she should not have more control over the EMR, and "…you leave chores like that to the people who have the responsibility and the training to do it," chores being controlling the privacy protection of EMR. Like Patient 34, Patients 8, 26 and 28 also reported that they would rather have the medical personnel control it because they trust them, and did not wish to obtain more control. Patient 7 claimed that if he or she had access to the EMR, he or she "…wouldn't know what to do with it." Patient 24 claimed to have no control and did not claim to seek any more control because no matter what the system could still be electronically hacked, and having more control would not stop the hacking. Patient 30 reported having no control because the physical EMR is on the physician's computers, not on his or her personal computer, and did not wish to obtain more control because that would only lead to an increased chance for potential breaches. Patient 42 claimed to have no control in the protection of the privacy of the EMR because of a lack of access to the system, and claimed "the only way that I would have control over my privacy is just not to say anything."

Of the 65% of patients who claimed to have no control in the protection of their records, 35% reported that they should have more control. Patient 10 sought out more control because he or she would "like to be the person most responsible for my life." Patient 17 wanted more control in the accessibility of his or her records. Most of the patients who reported having no control, but desired more control, desired such control in order to ensure the accuracy of the information in the record and for review purposes. Patients 13, 31, 36, 41, and 43 each felt this way, and Patient 36 claimed that he or she wanted to be able to "routinely access [his or her] records…

just to see if the doctors are putting in the right information, which in some cases they're not."

Patient 38 desired more control in order to see the results of tests in a more timely manner.

Patient 44 also reported having no control, and desiring more of it.

> I found out what I was going to need to go through in order to restrict access to my
>
> information, or at least the mental health stuff. It was just so complicated that it just
>
> wasn't worth it. And it should be the other way around… If I want to put my information
>
> out there, then I should have to go through the hassle to do that. (Patient 44)

Patient 44 wanted more control "to ensure that my mental health records were not accessible,

unless in an absolute emergency," expressing the dislike in having mental health information in

the same place as other medical information, and equally accessible. Patient 19 was the only

patient who claimed to have no control in protecting the information in the EMR and was unsure

in whether he or she should have more control "because I don't know what constitutes me having

more control."

Of the 34% of patients who claimed to have some or minimal control in the protection of

their records, 50% reported that they should not have more control. Patient 25 expressed having

more control than any other patient had expressed, and stated having "more than enough to

[protect the EMR]," and did not desire more control. Patients 12, 15, 20, and 39 each reported

having minimal or some control in the protection of privacy of the EMR, and the control to

which they referred was to the ability to control what they say and do not say to their providers.

Patient 20 did not desire any more control because he or she felt that the "doctors and nurses

know what they're doing; it's their job, not mine…." Patient 2 claimed to have some control

because he or she had been able to go into his or her records and remove information from them,

but continued to worry as he or she was aware that the EMR gets backed-up or archived. Patient 21 claimed to have some control and claimed, "…if I were more worried about [having control], I think I could probably have more. I'm just not sure how I'd go about it at this point, but I'm sure I could find out." The same patient did not wish to gain more control and stated, "I think that the assurances of the providers and the administrators… should be a pretty good idea of whether or not your information is safe." Patient 33 reported having minimal control as well and attributed his or her lack of wanting more control to the trust he or she in the physician.

> I think it's a question of being confident that the people I'm dealing with are professional and going to act accordingly… I'm confident enough in my doctor to say that he's going to do only what is in my best interest. It's a confidence type thing. Trust. (Patient 33)

> Of the 34% of patients who claimed to have some or minimal control in the protection of their records, 21% reported that they should have more control. Patient 4 reported having minimal control because, "I don't see myself being a big part of the loop [of information dissemination]… once it's been given, it's totally out of my hands," and desired more control in order to be able to review his or her medical information at will. Patient 11 also desired more control.

> People should be allowed to look at their record to assure that things have been transmitted appropriately… It might help because I think people would be actively engaged… in making sure that the information [in their record] is correct. They could see the thinking process of the clinician or the specialist that they consulted with. (Patient 11)

Patient 22 reported having minimal control in protecting the privacy in his or her EMR and desired more control "…because it's my medical record, I should have as much control over it that I feel that I should have."

Of the 34% who claimed to have some or minimal control in the protection of their records, 29% reported feeling unsure. Patient 17 claimed that because of its electronic nature, it is hard to maintain control of the files, and was unsure whether he or she desired more control because of not knowing what do with the files if more control was obtained. Patient 27 claimed to have some protective control, and stated, "The only way I can protect [my information] from them would be [to] not tell [my doctors]. And if you don't tell them, they can't make any decisions…" Patient 27 was also unsure how gaining more control over his or her records would benefit, stating, "I don't see how…. If you want the kind of medical care that you think you deserve… you're going to have to tell [your doctors] what you're problems are." Patients 29 and 32 each claimed they had minimal control as well, and were both unsure about what having more control over their medical records actually meant.

Chapter 4

Summary of Findings

The major benefits of the EMR reported by the interviewed patients included: accessibility of the medical information, speed at handling the system, efficiency, organization, and accuracy of inputted information, coordination of care across institutions and medical professionals, security of the system, and environmental benefit of paper reduction. The major problems associated with EMR according to the interviewed patients were: being error-prone, lack of user competence, time-management implications, and the largest issue of them all, security issues, which included miscommunication, loss of information, hacking, too much access, privacy and confidentiality concerns, and worry about inappropriate exposure.

After obtaining a general consensus as to what patients perceived the benefits and problems associated with EMR to be, patients reported how they perceived this novel technology to affect the doctor-patient relationship, if at all. A little more than one-third of the patients believed EMR to have a positive effect on the doctor-patient relationship in that EMR allows physicians to keep up with the information in the general field of medicine and the information regarding their specific patients, makes medical information more readily available, and facilitates the interaction between the physician and the patient. Just about one-third of the patients believed EMR to have a negative effect on the doctor-patient relationship. Here, EMR was perceived as having the potential to make physicians seem non-attentive and less personal due to their preoccupation with the computer during an actual clinical interaction with a patient. This observation led some patients to view EMRs as impersonalizing their interactions with

doctors; one-quarter of the patients claimed that EMRs had no effect on the doctor-patient relationship.

It was important to understand patient perceptions of EMR and its effect on the doctor-patient relationship before understanding the importance of trust in that relationship because trust has different interpretations in the medical context and is the foundation for privacy formations. Most patients reported trust to be very important in the doctor-patient relationship, claiming that trust will reflect in positive care. Patients claimed that they must trust the abilities of their physicians and trust whatever the physician says. Most patients also reported being able to completely trust their doctors, and attributed this trustworthiness to: the professionalism of the physician, inherent trust in the physician, amount of time spent with the physician, personality of the physician, and if the physician listens to the patient. Few patients claimed to have only limited trust or no trust in their doctors, and attributed this lack of trust to: poor relationships with their physicians, worry about inappropriate exposure of personal health information to others, and worry regarding the physician caring more about the clock than about the patient care.

In an attempt to understand patient's perceptions of privacy, patients were asked about their expectations and concerns regarding privacy in general. The major finding was that personal information should only be shared with other medical personnel once the patient has permitted the sharing of it. Some patients expected complete privacy, fewer patients expected to not be informally discussed, some had no privacy concerns (generally because those patients had nothing to hide in their records), and only a very small number of patients had low or no expectation of privacy.

When asked about expectations of privacy when medical personnel interacted, most patients expressed no concerns because they were confident that any interaction between medical personnel would be a positive collaboration that could only benefit patient care. The patients who did have concerns with their privacy when medical personnel interacted reported that way because they were worried about being inappropriately or informally discussed. Those patients believed that patient information should only be discussed between providers if the patient has previously permitted the disclosure of his or her personal information, and that discussions regarding patient information were better had behind closed doors and out of ear-shot of other patients and uninvolved medical personnel.

Then when asked about personal privacy concerns, most patients had none because they considered EMR to be safe, and simply desired the best care possible. However, a few patients did have concerns with the locations in which medical personnel discussed specific patient information, the potential for inappropriate sharing of personal information without patient consent, and with the privacy of personal information when shared with the insurance company.

In formulating definitions for privacy in relation to EMR, most patients were unable to come up with specific definitions, but instead were able to report what privacy was related to. Most patients defined privacy as being related to who has access to the EMR; patients also defined privacy in terms of: the medical records only being shared within the health care institution, the medical records being shared with only those who the patient has permitted, who has general access to the records, and the fact that there is the potential for too much access within the EMR. Few patients defined privacy in terms of the security of sensitive information in the EMR and some did not know what to say when asked.

Once the patients reported their definitions of privacy in relation to EMR, and their expectations and concerns regarding EMR, they then reported their perceptions of the effect of EMR on patient privacy. Most patients claimed that EMR makes personal information more accessible, thereby decreasing privacy, because of the possibility of medical personnel leaving the EMR screen open inappropriately for other, potentially unauthorized, personnel to view. Also, the EMR's online nature makes it more susceptible to hacking. Few patients claimed that EMR makes personal information less accessible, thereby increasing privacy. Those patients believed this because they considered a paper chart hanging outside of exam room door more vulnerable than information stored in an online system with protective mechanisms such as passwords, firewalls, and encryptions.

More than half of the interviewed patients reported that the exposure of personal information was more likely when using EMR rather than paper because of the existence of hackers, and because of the security concerns surrounding the concept of having a password to access information. Those patients who claimed that exposure was less or equally as likely to occur when using EMR reported this way because access to EMR is limited to medical personnel, protective mechanisms exist to protect the integrity and security of the EMR, and the physical nature of the EMR does not allow for its destruction via fire or other natural causes that can destroy paper.

When asked who or what patients believed to be the most responsible entity for ensuring the privacy of the EMR, a little more than one-third of the patients reported the hospital administration to be the entity most responsible, just about one-third of the patients reported the entity to be those who work in the medical records department, very few patients reported the

entity to be the physicians, even fewer reported the entity to be the patients or anyone who has

access to the records, and one patient reported the entity to be the insurance company. When

asked if their chosen entity was capable of protecting the privacy associated with EMR, most

patients reported their entity to be capable. Those who reported their entity to be the hospital

administration trusted that their privacy would be protected because of an inherent trust in the

system, also known as institutional trust. Those who reported their entity to be the physician

trusted that their privacy would be protected because of trust in their physician's training, also

known as interpersonal trust. Very few patients reported their entity to be incapable of protecting

the privacy of that EMR. Those who reported their incapable entity to be the hospital

administration did not trust that their privacy would be protected because of the large size of the

hospital and a lack of security of the EMR system, or institutional distrust.

Apart from responsibility and capability of ensuring the privacy protection of EMR,

commitment to that privacy protection was also discussed. Most patients reported that their

chosen entity would be committed to protecting the privacy of the EMR. Those who reported the

medical records department as being committed to privacy protection claimed that it was because

it is the job of the people who work in that department to protect the EMR's privacy, another

indication of institutional trust. The next largest number of patients reported feeling unsure, but

optimistic that their entity of choice would be committed in protecting the privacy of the EMR,

and a very small number of patients reported feeling that their entity of choice would be

uncommitted in protecting that privacy of the EMR.

The medical profession has been known to be one of the most autonomous professions;

however, the technological era in which we live has given rise to the increased autonomy of

patients and subsequent decrease in physician autonomy. That being said, patient control of their own records is another aspect of this technological change. Nearly two-thirds of the patients interviewed reported having no control in the privacy protection of their records in the EMR. Most of these patients reported that they should not have more control because either they would not know what to do with it, or they would not be able to stop the potential hacking of the system. Some of these patients reported that having more control would only lead to the increased likelihood for potential breaches. A smaller portion of patients who reported having no control in the privacy protection of their EMR reported that they should have more control in order to ensure the accuracy of the information in the EMR and for review purposes. One-third of the patients interviewed reported having some or minimal control in the protection of their records in the EMR. Half of those patients did not desire any more control; they were happy with the control they had, which was the ability to control what they do and don't say to their providers. Some did not desire more control because they believed that medical personnel knew what they were doing, indicating trust in the institution.

Relevance to the Literature

In her study, Nissenbaum (2004) discussed how EMR is a novel technology and with such a technology comes the inescapable unfamiliarly and confusion with the overall system and its capabilities. Interestingly, eleven years after the publishing of Nissenbaum's (2004) article, patients were indeed able to identify major benefits and concerns they perceived to be associated with EMR; however, patients identified the increased access generated due to EMR implementation to be both a benefit and a concern. Indeed, the literature has shown that the main

purpose of EMR is its increased accessibility (Barrows and Clayton 1996), but still many patients reported its increase in accessibility to be a negative aspect. These patients were mostly concerned with the online nature of the EMR and the security concerns that come along with such a system, including but not limited to hacking and inappropriate exposure; those concerns were not associated with negatively affecting the doctor-patient relationship, but instead associated with negatively affecting patient privacy by decreasing it. The possibility of a medical professional leaving the EMR screen open for others to inappropriately view, and the susceptibility of the EMR to hacking were the main concerns voiced by patients in terms of the EMR's affect on patient privacy, but were not concerns of how the doctor-patient relationship may change due to EMR implementation.

The literature also shows that privacy has been defined as an individual's ability to control the accessibility to his or her own medical records (Cantor 2006), which parallels the majority of privacy definitions reported by the patients. In addition, the literature notes how a major purpose of the EMR is to facilitate the sharing of information (Barrows and Clayton 1996), which a majority of patients had reported as being related to the definition of privacy in general. That being said, a major concern expressed by patients involved how their information was shared amongst their providers. When patients are not worried about inappropriate or public exposure, they are more likely to report more accurate information (Sankar et al. 2003). That dissemination of accurate information is the foundation of what medical professionals use to diagnose patients, or to figure out the next best course of action. Without giving accurate information, physicians would be unable to diagnose or treat properly, which would have a great potential of resulting in medical error. This is why it is important for medical professionals to

ensure that patients are not worried about the privacy (or lack thereof) of their information. A majority of the interviewed patients were found to be concerned with public exposure, and how their information is shared, claiming that they expected to be consulted with before a physician shares their information with another medical professional. This is an issue because if patients begin to doubt the privacy of their information, they may be less likely to be completely honest when consulting with their physicians. This worry, doubt, and misunderstanding of how information is shared was expressed by the interviewed patients, and has also been discussed in the literature. Patients reporting that they trust the practices of their health care system have also been found to be generally unaware, misinformed, and confused about the actual data sharing practices of heath care organizations (Goodwin et al. 2002).

On the other hand, most patients reported completely trusting their physicians because of the perception that trust will reflect in positive care. However, the literature has shown that when trust is referred to in the context of health, it is usually uncertain whether that trust is referring to the medical professional or to the medical institution (Brownlie 2008). When trust is referring to a health care professional, it can be called interpersonal trust, and when trust is referring to a health care institution, it can be called institutional trust. Interestingly, patients claimed to trust their physicians in terms of both types of trust. The interpersonal trust stemmed from the physician's professionalism, personality, and the ability to listen and spend time with their patients; the literature also directly states these reasons to be mechanisms of trust formation (Mechanic 1998). Patients also reported trusting their physicians simply because they had a medical degree and were employed by the hospital; this can be interpreted as those patients having institutional trust because they are putting their trust in the institution that hired those

physicians as opposed to the physicians themselves. This phenomenon was not discussed as much in the literature; however, the literature did mention that patients tended to have more interpersonal trust than institutional trust, something not necessarily seen in the patient data analyzed (Mechanic 1998).

Once the patient's trust in their physicians has been determined, it is possible to attempt to understand how the EMR affects the privacy of the doctor-patient relationship. Research has shown that trusting a new technology comes hand in hand with trusting that the institution has processes to ensure the competence of the people using the technology, and in the case of the EMR, to ensure the security of the information stored in that technology (Farquharson and Critchley 2004). Those patients who reported the EMR as having a negative effect on the doctor-patient relationship attributed their claims to physician non-attentiveness due to the staring at a computer screen rather than making eye-contact with the patient. The literature has shown how crucial eye-contact is in developing a trusting relationship (Mechanic 1998). However, the privacy aspect of the doctor-patient relationship is the concept that is becoming questioned with the implementation of the EMR, and the patient's worries about public or inappropriate exposure and lack of security mechanisms in place are the major concerns that have arisen due to this novel technology.

In her study, Merisalo (2012) found that patients who have online access to their EMR find benefits in having the control to find and correct errors in their records, in the ability to better understand their health conditions, and in being able to keep up with their medications. Although many interviewed patients had never had access to their own records, some reported that having said access would increase their control, thereby increasing their patient autonomy,

their comfort with the use of EMR, and the protection of their privacy. That being said, most patients claimed to have no control over the privacy of their medical records, and did not desire to obtain control because they would not know what to do with it and would not be able to stop any potential hacking of the system, paralleling the findings of Merisalo's (2012) study. Like Annas' (2003) study showed, few patients reported that most of the control in protecting the privacy of their records came from what they chose to disclose and what they chose not to disclose to their physicians.

It is imperative to discuss the person or entity that is most important in terms of dealing with the privacy of the information in the EMR. The literature mostly discussed this entity being the physician, as the physician's management of personal information is considered an aspect of trust in the context of the medical field (Mechanic 1998). Interestingly, the patients interviewed in this study reported many more entities than just the physician at being most responsible for protecting the privacy of the EMR. The patients who reported the hospital administration or the medical records department to be the entity most responsible for protecting the privacy of the EMR also reported them being capable of and committed to protecting that privacy because of an inherent trust in the system, or institutional trust. The patients who reported the physician to be the entity most responsible for protecting the privacy of the EMR also reported them being capable of and committed to protecting that privacy because of their training as a physician, or interpersonal trust.

Discussion

Before health information technology existed, patients would walk into their doctor's office, fill out some forms in the waiting room, wait to be called into the doctor's office, and sit in the office for a few minutes. Then, the doctor would enter the office holding the patient's paper file in hand. The physician and the patient would talk for a few minutes, devise a plan of action, while the physician took notes, in the patient's tangible paper file, with a pen. Nowadays, paper files are becoming obsolete as the health care field transitions from paper to electronic records. Today, when patients walk into their doctor's office, they may or may not have to fill out certain forms, and still wait to be called in, but now when the doctor enters his or her office, he or she is no longer accompanied by a physical, tangible paper file, but a laptop computer programmed with EMR software. The doctor no longer takes notes with a pen on blank paper, but uses a keyboard to input notes onto templates. This seemingly minute difference in the medical record's nature has outstanding impacts on the ways in which patients interact with their physicians and their medical institutions as a whole, and the ways in which they perceive privacy at both the micro level, within the doctor-patient relationship, and at the macro level, within the health care institution.

Perception is the way in which one interprets a situation. If I was walking down the street and saw a man and a woman engage in a hug, I might think that those two individuals are happy to see each other. However, those two people may be hugging because someone close to them has just passed away, and are embracing each other because of a shared sense of sadness and mourning. Because I am not associated with those people, I perceive their interaction as a happy interaction when their interaction was in fact a sad interaction. The subjective nature of human

thought and action has been a prominent topic in the history of sociological thought (Merton 1995). It was at the beginning of the 20th century when W. I. Thomas and Dorothy Swaine Thomas developed "the Thomas Theorem" (Merton 1995: 380). The basis behind their theorem was that "'if men define situations as real, they are real in their consequences'" (Thomas and Thomas 1928: 572 as stated in Merton 1995).

The Thomas Theorem is applicable to my thesis topic for a variety of reasons. Since the beginning of health care, patients have always been able to subjectively formulate their perceptions regarding privacy, but it is in this technological era that those perceptions have the potential to change. It is important to understand how patients perceive their privacy in the field of health care because if patients are not completely comfortable with the privacy of their information in a heath care setting or within the doctor-patient relationship, they are much more likely to withhold information regarding their health, which may prevent physicians from doing their jobs to the best of their abilities (Caine and Hanania 2012; Goodwin et al. 2002).

Applying the Thomas Theorem, we might then conclude that 'if patients perceive their privacy as protected, then their privacy is protected'. Accordingly, 'if patients perceive their privacy as not protected, then their privacy is not protected'. Thomas' Theorem claimed that perception is reality; therefore, in order to determine how patients perceive their privacy and the ways in which the implementation of EMR shapes those perceptions, we need to know what their perceptions are.

In 1937, Herbert Blumer coined the term symbolic interactionism, which is a micro level theory that deals with the idea that "human beings have the capacity to think and decide on their own how they should act in given situations, and that they react on the basis of their perceptions

and definitions of the situations in which they find themselves" (Delaney 2014: 176 and 255).

Beginning from first-impressions, patients and doctors develop perceptions of each other while they interact. These perceptions are crucial because of the trustworthy and private nature of the doctor-patient relationship. The trust that is referred to when a patient trusts their doctor is known as interpersonal trust, and without the development of this trust, patients will be unable to trust their doctors in protecting the privacy of their information.

Because of the implementation of EMR, physicians are now mostly accompanied by their laptops. Presently, when patients interact with their physicians, they claim that the doctor-patient relationship has lost some of its value because of the "staring-at-the-screen" phenomenon or because of the impersonal nature of the interaction due to the laptop's presence. The staring-at-the-screen phenomenon was reported by many patients in this study and occurs when physicians interact with their patients. Instead of making eye-contact with their patients, physicians who are unaccustomed to electronically recording information may only be making eye-contact with the computer screen. Eye-contact indicates listening, and listening is a key component in the development of a trustworthy relationship, particularly in the doctor-patient relationship (Mechanic 1998). The reason physicians stare at their screens may be due to their unfamiliarity with the EMR system; they may need to fixate their eyes on the screen so that they do not mistakenly input information into a place where that information does not belong. Information inputted into a wrong section of the EMR may have the potential to be edited and corrected, but by not making eye-contact with their patients, physicians may be unable to establish trust with their patients, and the doctor-patient relationship has the potential to become increasingly impersonal.

Another important factor in the establishment of interpersonal trust within the doctor-patient relationship is knowing why patients trust their doctors. Patients in this study reported trusting their physicians because of their professionalism, knowledge, intelligence, skill, competence, honesty, and respectfulness. Each of those qualities refers to the actual physician, which is why this type of trust is referred to as interpersonal. When asked about whether their physician was able to ensure and protect the privacy of their personal information stored in the EMR, patients claimed that their physicians were, in fact, able to do so because they trusted the training of their physicians, another indication of interpersonal trust.

Perceptions of interpersonal trust also shaped patient's perceptions of privacy. Most patients defined privacy not only as related to who has access to their EMR, but the way those patients perceived that privacy within the doctor-patient relationship. For example, patients expressed concerns regarding who their information was being shared with and why, and of not wanting it to be informally discussed by their health care providers, be it inside or outside of the health care setting. Patients perceived their privacy as being protected by their physicians only if they trusted their physicians to consult with them prior to sharing any personal information, and if they trusted them to avoid informally discussing any aspect of their medical records.

Similarly, patients also reported concerns about the increased access of information offered by the use of the EMR. It was believed that its online nature may make the EMR more susceptible to hacking from outside sources. Patients also believed there there was the potential that medical personnel might leave the EMR screen open (not properly logging out), revealing their health information to potentially unauthorized personnel to view. Not trusting the medical professional at being capable of properly logging out of the EMR can be considered a form of

interpersonal distrust. That being said, not trusting the EMR and its protective mechanisms, such as its passwords, firewalls, and encryptions, to protect the information in the system can be considered to be a form of technological distrust, or, on a macro scale, institutional distrust.

Research has shown that patients tend to have more interpersonal trust than institutional trust (Mechanic 1998). Institutional trust is important because without it, patients would be unable perceive their personal health information as protected, and if they cannot trust their information to be protected by the system, they would be less likely to be completely honest with their providers. Many patients in this study reported trust to be of extreme importance, and while further discussing trust, many patients reported trusting their physicians simply because they are doctors. When patients claim to trust their physicians because of an inherent trust, or a blind trust, they are actually putting their trust into the institution because the institution essentially accredits those physicians.

When differentiating between interpersonal and institutional trust, the entities in which patients put their trust are separated into individuals and institutions. One of the patients who was interviewed, commented that he or she had changed his or her provider from an older physician to a younger physician because the older physician was unable to open the patient's CT scan in the EMR, which made the patient incredibly uncomfortable and scared, so much so that she changed her provider to a younger more "tech savvy" physician. After watching the older physician being unable to work with the EMR, the patient lost trust in that physician and subsequently changed providers, representing interpersonal distrust. However, some patients were uncomfortable with the increased accessibility associated with the EMR, and if those patients were unable to trust the physical technology of the EMR system, they would be

experiencing institutional distrust, and would no longer perceive their personal health

information as being private.

Many patients reported the entity most responsible for ensuring the privacy of the

information stored in the EMR to be either the hospital or the medical records department.

Interestingly, the patients who reported the entity to be the hospital simply said the hospital, but

when asked to further their responses, they referred to the hospital as the hospital administration

without explicitly saying it. They made it seem like the physical hospital building was

responsible for ensuring and protecting the privacy of the EMR, as opposed to the people who

run the hospital. Thus, those patients were trusting the institution which houses their health

information. The other set of patients who reported the medical records department as the entity

most responsible for ensuring the privacy of the EMR were also putting their trust in the

institution. Some of the patients who reported the entity to be the medical records department

may, however, not have known if such a department even existed. Many patients did not

elaborate on why they chose the medical records department and simply stated that the people

who work in said department are smart people with good intentions. Perhaps these patients

reported with abstractions that they constructed in order to make themselves feel more secure. Is

this medical records department located in the hospital? Is there a giant vault full or servers with

armed guards at the entrance? I do not know the answers to those questions, and I do not think

the patients knew the answers either.

Interestingly, when patients were asked about their perceptions regarding how much

control they had over the protection of their records, many of them reported having some or

minimal control. When asked if they desired more control, many of those patients reported to not

want more control because they believed that the medical personnel who currently control the EMR know what they are doing, thus trusting the institution to control their EMRs.

A good example of the converging of micro and macro perceptions of interpersonal and institutional trust is within the expectations and concerns regarding privacy. We have already discussed those perceptions that develop within the doctor-patient relationship, but the perceptions that develop when medical personnel interact portray the difficulty in determining a perception to be related to interpersonal or institutional trust. It is the trust in the person or the system that is the foundation of the privacy perception.

Medical personnel interact with each other and discuss patients all day long. Many of the patients interviewed expressed no concerns regarding their privacy when medical personnel interact because they believed that collaboration would only result in the betterment of care. On the other hand, many patients were concerned with their privacy because they worried about being inappropriately discussed, and about whether the conversation between those providers was occurring within earshot of other patients or anyone who should not be involved in the discussions of that patient. Concerns about being inappropriately discussed were not original concerns. In Ubel et al.'s (1995) study, researchers stood in hospital elevators to see how much inappropriateness existed in conversations between medical personnel. The study found a remarkable amount of inappropriate comments including comments that violated patient privacy, and comments that were derogatory towards patients (Ubel et al. 1995).

Patients may perceive their privacy as being violated for completely two different reasons. The violation of privacy may be because of the medical personnel who should be more aware of their surroundings and should only discuss patients behind closed doors, or the

violation of privacy may be because the hospital that should have better mechanisms in place to ensure that medical personnel are more careful when discussing patients. The first perception is formed based on a lack of interpersonal trust, and the second perception is formed based on a lack of institutional trust. Although the concern exhibited by the patients was "inappropriate discussion or private information," that concern may be perceived from two different vantage points. This is where the Thomas Theorem can be applied; it is all about the way a situation or concern is perceived in determining the concrete perspectives that develop.

Conclusion

From the macro standpoint of trusting the institution, the EMR seems to play less of a role in patient's perceptions of privacy than it does from the micro standpoint of trust within the doctor-patient relationship. The EMR changes the doctor-patient interaction by making it more impersonal; the physician has a tendency to stare at the computer screen, thereby avoiding eye-contact and subsequently losing patient trust. Although patients mostly reported trusting their doctors in protecting the EMR that stores personal health information, they had less trust in the EMR system as a whole, claiming that the EMR increases accessibility to the information stored in it. Patients can trust their physicians as much as they want, but if they do not have trust in the EMR system to protect their privacy, the doctor-patient interaction becomes uncertain and less trustworthy. Therefore, on the micro level, patient's perceptions of privacy are more greatly influenced by the EMR than the medical professional.

On the macro level, the formation of patient privacy depends on the trustworthiness of the institutions that house the EMR systems. Patients did report to trust the institutions to ensure

and protect the privacy of the information stored in the EMR, but many patients seemed to be making comments based on how they perceived their privacy in being protected. However, only a very few knew exactly how that was done. Regardless, patients placed their trust in the hospital and the medical records department to secure the privacy of their information, but the online nature of the EMR caused patients to feel as if their information was vulnerable to a breach, hacking of the system, or vulnerable to incapable medical personnel who may leave the EMR screen open for unauthorized viewing. Either way, the online nature of the EMR altered the way patients perceived the security of their information.

In order to obtain the best care possible from their providers, patients must be able to trust their physicians, trust the EMR, and trust the health care institution. The advent of the electronic medical record system has most certainly played a pivotal role in the establishment of patient's perceptions of privacy.

Study Limitations and Future Research

One limitation of this study was the population of patients interviewed. The patients who participated in this study came from one of two hospitals in the northeastern region of the United States. It is quite possible that the results of this study may have been different if the participants were from different hospitals in different parts of the United States. As such, we can not make generalizations to other patient populations or groups. Nevertheless, the information presented in this paper can be very useful in helping to reshape the field of medicine. The medical field is changing because of the technological advancement of EMR and its implementation. Once patients are able to fully trust the EMR system and the privacy protection of their personal health

information within the system, the likelihood of patients withholding information from their

providers will decrease, and physicians will be better able to diagnose, treat, and cure their

patients. Because of the technological era in which we live, it can be assumed that other

technologies, like EMR, will be introduced into the field of medicine in the future, and due to

this study, we will know what to do to ensure privacy and trust in those technologies and the

providers who utilize them.

References

AlHamad, Ahmad Q., Faruq A. Omari and Asma Q. AlHamad. 2014. "Recommendation for Managing Patients' Privacy in an Integrated Health Information Network." *Journal of Information Technology and Economic Development* 5(1):47.

Annas, George J. 2003. "HIPAA Regulations--A New Era of Medical-Record Privacy?" *New England Journal of Medicine* 348(15):1486.

Baker, Robert. 2013. *Before Bioethics: A History of American Medical Ethics From the Colonial Period to the Bioethics Revolution.*United States of America: Oxford University Press.

Barrows, R. C.,Jr and P. D. Clayton. 1996. "Privacy, Confidentiality, and Electronic Medical Records." *Journal of the American Medical Informatics Association : JAMIA* 3(2):139-148.

Blumenthal, David and Marilyn Tavenner. 2010. "The "meaningful use" Regulation for Electronic Health Records." *New England Journal of Medicine* 363(6):501-504.

Brownlie, Julie. 2008. "Conceptualizing Trust and Health." *Researching Trust and Health* 1:17.

Caine, K. and R. Hanania. 2013. "Patients Want Granular Privacy Control Over Health Information in Electronic Medical Records." *Journal of the American Medical Informatics Association : JAMIA* 20(1):7-15.

Cantor, Michael D. 2006. "No Information about Me without Me: Technology, Privacy, and Home Monitoring." *Generations* 30(2):49-53.

Damschroder, Laura J., Joy L. Pritts, Michael A. Neblo, Rosemarie J. Kalarickal, John W. Creswell and Rodney A. Hayward. 2007. "Patients, Privacy and Trust: Patients' Willingness

to Allow Researchers to Access their Medical Records." *Social Science & Medicine* 64(1): 223-235.

Davis, L., J. A. Domm, M. R. Konikoff and R. A. Miller. 1999. "Attitudes of First-Year Medical Students Toward the Confidentiality of Computerized Patient Records." *Journal of the American Medical Informatics Association : JAMIA* 6(1):53-60.

Delaney, Tim. 2014. *Classical and Contemporary Social Theory, Investigation and Application*. New York: Oxford University Press.

Dew, Kevin, Sonya Morgan, Anthony Dowell, Deborah McLeod, John Bushnell and Sunny Collings. 2007. "'It Puts Things Out of Your Control': Fear of Consequences as a Barrier to Patient Disclosure of Mental Health Issues to General Practitioners." *Sociology of Health & Illness* 29(7):1059-1074.

Farquharson, Karen and Christine Critchley. 2004. "Risk, Trust and Cutting Edge Technologies: A Study of Australian Attitudes." *Australian Journal of Emerging Technology and Society* 2(2):124-146.

Gaylin, Daniel S., Adil Moiduddin, Shamis Mohamoud, Katie Lundeen and Jennifer A. Kelly. 2011. "Public Attitudes about Health Information Technology, and its Relationship to Health Care Quality, Costs, and Privacy." *Health Services Research* 46(3):920-938. doi: 10.1111/j. 1475-6773.2010.01233.x.

Gilding, Michael and Christine Critchley. 2003. "Technology and Trust: Public Perceptions of Technological Change in Australia." *Australian Journal of Emerging Technology and Society* 1(1):52-69.

Goodwin, Linda, K. Courtney, JD Kirby, MA Iannacchione and T. Manley. 2002. "A Pilot Study: Patients' Perceptions about the Privacy of their Medical Records." *Online Journal of Nursing Informatics* 6(3).

Hall, Mark A., Elizabeth Dugan, Beiyao Zheng and Aneil K. Mishra. 2001. "Trust in Physicians and Medical Institutions: What is it, can it be Measured, and does it Matter?" *Milbank Quarterly* 79(4):613-639.

Hall, M. A., B. Zheng, E. Dugan, F. Camacho, K. E. Kidd, A. Mishra and R. Balkrishnan. 2002. "Measuring Patients' Trust in their Primary Care Providers." *Medical Care Research and Review : MCRR* 59(3):293-318.

Kass, Nancy E., Marvin R. Natowicz, Sara C. Hull, Ruth R. Faden, Laura Plantinga, Lawrence O. Gostin and Julia Slutsman. 2003. "The use of Medical Records in Research: What do Patients Want?" *The Journal of Law, Medicine & Ethics* 31(3):429-433.

Mandl, Kenneth D., Peter Szolovits and Isaac S. Kohane. 2001. "Public Standards and Patients' Control: How to Keep Electronic Medical Records Accessible but Private." *BMJ: British Medical Journal* 322(7281):283-286.

McGraw, D., J. X. Dempsey, L. Harris and J. Goldman. 2009. "Privacy as an Enabler, Not an Impediment: Building Trust into Health Information Exchange." *Health Affairs (Project Hope)* 28(2):416-427.

Mechanic, D. 1998. "The Functions and Limitations of Trust in the Provision of Medical Care." *Journal of Health Politics, Policy and Law* 23(4):661-686.

Merisalo, Laura J. 2012. "Protecting Patient Privacy: Patients Value Electronic Health Records, but Worry about Data Breaches." *Healthcare Registration* 21(7):1.

Miller, Amalia R. and Catherine Tucker. 2009. "Privacy Protection and Technology Diffusion: The Case of Electronic Medical Records." *Management Science* 55(7):1077-1093.

Merton, Robert K. 1995. "The Thomas Theorem and the Matthew Effect." *Social Forces* 74:379-422.

Nissenbaum, Helen. 2004. "Will Security Enhance Trust Online, Or Supplant it." *Trust and Distrust within Organizations: Emerging Perspectives, Enduring Questions*:155-188.

Pyper, C., J. Amery, M. Watson and C. Crook. 2004. "Access to Electronic Health Records in Primary Care-a Survey of Patients' Views." *Medical Science Monitor : International Medical Journal of Experimental and Clinical Research* 10(11):SR17-22.

Sankar, Pamela, Susan Mora, Jon F. Merz and Nora L. Jones. 2003. "Patient Perspectives of Medical Confidentiality." *Journal of General Internal Medicine* 18(8):659-669.

Slutsman, J., N. Kass, J. McGready and M. Wynia. 2005. "Health Information, the HIPAA Privacy Rule, and Health Care: What do Physicians Think?" *Health Affairs (Project Hope)* 24(3):832-842.

Sobel, Richard. 2007. "The HIPAA Paradox: The Privacy Rule that's Not." *Hastings Center Report* 37(4):40-50.

Ubel, Peter A., Margaret M. Zell, David J. Miller, Gary S. Fischer, Darien Peters-Stefani and Robert M. Arnold. 1995. "Elevator Talk: Observational Study of Inappropriate Comments in a Public Space." *The American Journal of Medicine* 99(2):190-194.

Von Staden, Heinrich. 1996. "In a Pure and Holy Way: Personal and Professional Conduct in the

    Hippocratic Oath?" *Journal of the History of Medicine and Allied Sciences* 51(4):404-437.

Williams, Arthur R., David C. Herman, James P. Moriarty, Timothy J. Beebe, Sandra K.

    Bruggeman, Eric W. Klavetter, Paul H. Steger and Janet K. Bartz. 2008. "HIPAA Costs and

    Patient Perceptions of Privacy Safeguards at Mayo Clinic." *Joint Commission Journal on*

    Quality and Patient Safety 34(1):27-35.

Zarcadoolas, Christina, Wendy L. Vaughon, Sara J. Czaja, Joslyn Levy and Maxine L. Rockoff.

    2013. "Consumers' Perceptions of Patient-Accessible Electronic Medical Records." *Journal*

    of Medical Internet Research 15(8):e168. doi: 10.2196/jmir.2507.