

Andrews University

Digital Commons @ Andrews University

Dissertations

Graduate Research

2007

The Health of Patient Privacy: The Patient's Perspective on the HIPAA Protected Health Information

Deborah Lange-Kuitse

Andrews University, deborahl@andrews.edu

Follow this and additional works at: <https://digitalcommons.andrews.edu/dissertations>



Part of the [Health and Medical Administration Commons](#)

Recommended Citation

Lange-Kuitse, Deborah, "The Health of Patient Privacy: The Patient's Perspective on the HIPAA Protected Health Information" (2007). *Dissertations*. 1699.

<https://digitalcommons.andrews.edu/dissertations/1699>

This Dissertation is brought to you for free and open access by the Graduate Research at Digital Commons @ Andrews University. It has been accepted for inclusion in Dissertations by an authorized administrator of Digital Commons @ Andrews University. For more information, please contact repository@andrews.edu.

ABSTRACT

THE HEALTH OF PATIENT PRIVACY: THE PATIENT'S
PERSPECTIVE ON THE HIPAA PROTECTED
HEALTH INFORMATION

by

Deborah Lange-Kuitse

Chair: Lyndon Furst

ABSTRACT OF GRADUATE STUDENT RESEARCH

Dissertation

Andrews University

School of Education

Title: THE HEALTH OF PATIENT PRIVACY: THE PATIENT'S PERSPECTIVE
ON THE HIPAA PROTECTED HEALTH INFORMATION

Name of researcher: Deborah Lange-Kuitse

Name and degree of faculty chair: Lyndon Furst, Ed.D.

Date completed: November 2007

Problem

As healthcare entities continue to focus on HIPAA compliance, they must enforce policies that require patients to sign and express understanding of the organization's privacy policies. It appears the patient's perspective on healthcare privacy has not been considered within the HIPAA privacy ruling. Patients are healthcare consumers, yet little research has been done on assessing the individual consumer's perspective on what Protected Health Information (PHI) is actually important to protect and from whom it is important to protect it.

Method

A quantitative survey was developed and distributed to the participants of the Carnegie group, an independent insurance firm in Chicago, Illinois. Inferential and descriptive statistics were used to analyze the differences and interactions among the participants based on 4 independent variables and 17 selected dependent variables.

Results

The analysis showed that of the 17 PHI indicators, only 5 of them were identified as being important to protect from healthcare providers. A One-Way Analysis of Variance was used to test for significant differences among the age and gender groups for each PHI indicator.

Analysis of the data on age showed the desire for privacy each respondent gave, and the data showed significance for the age group 31-45. This group desired more privacy than any other group. The age group 18-30 scored the lowest on privacy concerns for each PHI. Gender differences showed males desire more privacy than females. The analysis on financial commitment given by the patient for each PHI showed no respondents placed a high dollar value on protecting the PHI indicators.

Two-Way Analysis of Variance was used to determine the main effect and interaction effect of age and authority on access of health information. The findings showed that the more authority granted to a doctor, the more likely a participant was willing to give healthcare information.

Conclusion

Overall, patients put little value in protecting the defined PHI as defined by the HIPAA privacy ruling from healthcare providers and are not willing to pay for privacy protection. Patients practice transparency with healthcare providers for much of the PHI, and only 5 PHI indicators were considered important enough to limit access by healthcare providers.

Andrews University

School of Education

THE HEALTH OF PATIENT PRIVACY: THE PATIENT'S
PERSPECTIVE ON THE HIPAA PROTECTED
HEALTH INFORMATION

A Dissertation

Presented in Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy

by

Deborah Lange-Kuitse

November 2007

© Copyright by Deborah Lange-Kuitse 2007
All Rights Reserved

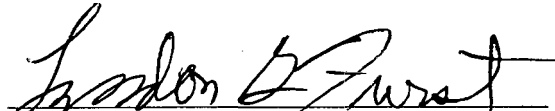
THE HEALTH OF PATIENT PRIVACY: THE PATIENT'S
PERSPECTIVE ON THE HIPAA PROTECTED
HEALTH INFORMATION


A dissertation
presented in partial fulfillment
of the requirements for the degree
Doctor of Philosophy

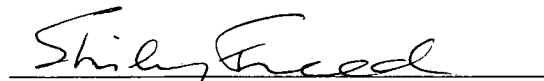
by

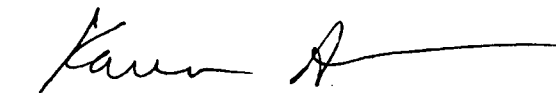
Deborah Lange-Kuitse


APPROVAL BY THE COMMITTEE:


Chair: Lyndon Furst


Dean, School of Education
James R. Jeffery


Member: Shirley Freed


Member: Karen Allen


External Member: Lowell Hamel

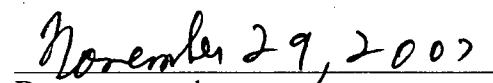

Date approved

TABLE OF CONTENTS

LIST OF TABLES	v
ACKNOWLEDGMENTS	vi
Chapter	
1. INTRODUCTION AND STATEMENT OF PROBLEM	1
Introduction	1
Information Sharing and Privacy	2
HIPAA Privacy Rule Component.	5
Statement of the Problem	8
Purpose of the Study	9
Research Questions	10
Theoretical Framework	11
Healthcare Transparency	21
Risk Adverse	23
Significance of the Study	24
Definition of Terms	26
Delimitations of the Study	27
Organization of the Study	28
2. LITERATURE REVIEW	29
Origin of Privacy	30
Key Privacy Legislation.	40
Key Judicial Cases and Legislation Related to Privacy.	40
Notable Supreme Court Cases Related to Privacy	45
Healthcare and Privacy	51
Transparency	66
Key Judicial Cases Related to Transparency	67
Feedback Regulations and Transparency	70
Independent Research and Transparency	71
Privacy Versus Transparency	75
Summary	81
3. METHODOLOGY	85

Research Design	86
Population and Sample	86
Instrumentation	88
Data Gathering	90
Pilot Study.	91
Research Questions	95
Analysis of Data	96
Limitations of the Study.	99
Summary	99
4. RESULTS	100
Research Question 1	102
Research Question 2	106
Research Question 3	113
Research Question 4	122
Research Question 5	123
5. SUMMARY, CONCLUSIONS, AND RECOMMENDATIONS	127
Theoretical Basis for the Study	127
Related Literature	130
Methodology	137
Summary of Findings	139
Conclusions	147
Recommendation for Further Research	149
Recommendation for Public Policy	151
APPENDIX: HEALTHCARE PRIVACY SURVEY	155
REFERENCE LIST	162
VITA	171

LIST OF TABLES

1. Percentage Scores by Gender and Age on Protection of Private Information . . .	73
2. Survey Demographic Results	102
3. Components of PHI that Patients Want Healthcare Providers to Have Access To.	105
4. ANOVA for Hypothesis 1—Age	108
5. Tukey HSD—Privacy Desired for Each PHI by Age Group	109
6. ANOVA Hypothesis 2—Gender	112
7. Mean Score—Healthcare Information Access	115
8. ANOVA for Hypothesis 3—Access by Individual to Healthcare Information Based on Authority Given to Doctor	116
9. Tukey HSD Test With Significance of .01—Significant Other	117
10. Tukey HSD With Significance of .01—Child	119
11. Tukey HSD With Significance of .01—Law Enforcement	119
12. Tukey HSD With Significance of .01—Pastor Religious Advisor	120
13. ANOVA for Hypothesis 4—Age Groups and Healthcare Access	121
14. ANOVA for Hypothesis 5—Interaction Between Authority and Age Regarding Access	122
15. Frequency Distribution for Dollar Value on Each PHI	124

ACKNOWLEDGMENTS

Many people endured, so others would gain. I am fortunate in my life to have many positive influences and support structures. Many people during this process made me laugh, dance, live, and sing. I wish to thank most of all Roelf S. Kuitse, my dearest friend, for all the days he spent alone and carried the family duties while I worked on my research. I wish to thank Roelf David Kuitse and Reanna Kuitse—my dearest children—for all their patience with me, their mom, and chili soup suppers, so I could commit myself to building my healthcare transparency theory.

I was blessed to have mentors in my life during the dissertation process, and I want to thank Bill Morelan for his guidance as he provided me with “editorial tutelage.” He was truly a friend and mentor. I also want to acknowledge Dr. Lyndon Furst, my Committee Chairman. He gave me wisdom and imposed challenges of thought. Thank you for the patience and endurance you showed me, and thank you for postponing your retirement until I was completed. You are a man truly dedicated to advancing education and improving public policy.

My final acknowledgments go to the Carnegie Financial Insurance group; this research data would not have been possible without the assistance of the Carnegie team and all the willing participants of the study.

I thank all of you who read this dissertation and take the knowledge contained within these pages and further the research to advance the healthcare system within our country, within our world.

CHAPTER ONE

INTRODUCTION AND STATEMENT OF PROBLEM

Introduction

Personal privacy has been described as “the most comprehensive of rights and the most valued by civilized men” (*Olmstead v. United States*, 1928, p. 438). Protection of personal information has been expressed as a high value in American society (Gray-Lukkarila, 1997). Individual privacy rights are also implied within the United States Constitution, and more specifically within the Bill of Rights.

The term *privacy* has been defined in many different ways. Some assert that privacy is the “right of the individual to determine when, how, and to what extent there should be a disclosure of information about himself” (AEI Legislative Analyses, 1997). Others say privacy can be seen “as creating the context in which both deceit and hypocrisy may flourish” (Schoeman, 1984, p. 1). Privacy can both expand as well as restrict personal and social well-being.

A key component of the American healthcare system is the ability to exchange private healthcare information within the system. Healthcare entities utilize information system technology in hospitals, physician offices, and clinics to maintain patient records, conduct patient billing, and manage patient workflow. The passing of personal healthcare information between provider, payer, and healthcare professional has become a routine part of rendering medical care.

Yet when patients come to receive care within a healthcare setting, their primary concern is not the privacy of their personal healthcare information. Rather they are consumed with the illness at hand and want to receive treatment that will cure them of their ailment (P. Peters, personal communication, October, 14, 2002). If patient-specific information is not given to the wrong person(s), the patient does not feel concern. However, if sensitive patient information is given to the wrong person(s), a patient may feel violated and mistreated.

Information Sharing and Privacy

The American healthcare industry relies on information system technology to give effective care (McKesson, 2000). Healthcare professionals share information with each other in order to render effective patient care, conduct research, and counsel family members. Healthcare providers pass information to payers in order to receive reimbursement for services rendered. The healthcare industry has become a collection of complex social structures, all collectively relating to each other in order to meet social demands for high-quality, cost-effective patient care (Tufts Managed Care Institute, 1998).

Social demands for high-quality care have economic ramifications as well. By 1997 the U.S. population was consuming 14% of the Gross National Product on healthcare (Docteur, Suppanz, & Woo, 2003). One intent of the 1997 Balanced Budget Act (BBA) was to decrease this \$1.2 trillion price tag for healthcare (Ross, 1999).

The BBA has brought about significant changes in the healthcare industry. Healthcare enterprises have scrambled to find ways to become more efficient while maintaining positive revenue streams and retaining quality healthcare for the populations

they serve. The leaders within healthcare organizations regularly look to technology to provide the efficiencies and cost-effective solutions necessary to cut costs and increase revenues, while streamlining healthcare practices (McKesson, 2000).

The advancement of the Internet and information systems technology has paralleled the growing need to constrain healthcare costs. Information systems technology and its applied uses within business, healthcare, and third-party payer groups have significantly increased the value of information. Healthcare enterprises are now able to collect data from different computer applications and aggregate the data to create powerful information packages. But the same information can be used to improve or to violate human well-being.

A 1992 opinion survey found that 79% of Americans agreed that “computers have improved the quality of life in our society” (Equifax, 1992, p. 4). Yet more recently, patient awareness of personal information vulnerability has come into focus due to the increased use of information system technology (Borgstede-Mason, 1999) and media coverage of abuses. Violations occurring with credit card fraud and financial credit reports, as well as intrusion into personal privacy via the Internet, have added to consumer concern about the need for personal information protection (Hendersen, 1999).

Patient-specific information is vulnerable to human error, outside intrusion, and abuse every day. Surgical schedules have been faxed to hotel receptionists by mistake. Hospital employees have accessed a friend’s healthcare information out of concern for their health status. Curious employees have checked someone’s account to see if they are receiving care in a psychiatric unit (McKesson, 2000).

The incident that occurred at the University of Michigan Health System (“Privacy Concerns”, 1999) where hundreds of patient names and diagnoses were accidentally released from the hospital’s information system to the Internet was not an isolated case. During the summer of 2000, more than 5,000 patient records were downloaded by a computer hacker from the University of Washington Medical Center’s administrative databases (Poulsen, 2000). Such incidents illustrate great potential for harm and the need for security with information.

As clinicians and other healthcare professionals began to utilize technology to make care decisions, conduct research, manage patient visits, and manage patient reimbursement, public concerns over providing privacy and security of healthcare data began to grow. The government responded to these concerns by extending the Health Insurance Portability Accountability Act 1996 (HIPAA) to include privacy and security of patient data under the HIPAA regulation (Kennedy-Kassebaum, 1996).

The Health Insurance Portability Accountability Act (HIPAA) of 1996—also known as Kennedy-Kassebaum Bill (Kennedy-Kassebaum, 1996)—put into motion the most sweeping legislation to affect healthcare since the installment of Medicare in 1965. The privacy component of the HIPAA regulation outlines 18 required “Protected Health Information Indicators” that healthcare entities are now required to protect.

The HIPAA regulation has multiple parts. The initial legislation was passed in 1996 with the three primary objectives of assuring health insurance, reducing healthcare fraud and abuse, and enforcing standards of health information. Additional provisions providing for “privacy” of health information were enacted in 2001, and “security” of

health information provisions were enacted in 2003. Together these five provisions are defined as the "Administrative Simplification."

One of the stated purposes of the new HIPAA provisions was to improve the efficiency and effectiveness of healthcare systems by standardizing the electronic exchange of administrative and financial data. In addition, the new HIPAA provisions were to provide a means to keep transmitted and electronically stored information private and secure.

These new provisions also required the Department of Health & Human Services (DHHS) to adopt national standards for electronic administrative and financial healthcare transactions. All health plans, all clearinghouses, and those providers who choose to conduct these transactions electronically are now required by federal law to implement these standards. Failure to comply with the adopted standards carries civil and criminal penalties for wrongfully disclosing confidential information.

HIPAA Privacy Rule Component

The privacy rule component of the HIPAA Administration was put into effect in the spring of 2001 (Kennedy-Kassebaum, 1996). The philosophy behind the privacy rule was "to provide an opportunity for and to encourage more informed discussions between patients and providers about how Protected Health Information will be used and disclosed within the healthcare system" (Federal Register 65, 2000, p. 82,474).

Congress mandated that the privacy rule be fully operational in every healthcare entity by 2003. (Some allowances were made for those entities that negotiate and contract with third-party entities.) The stated intent of the Privacy legislation was to restrict unauthorized use or disclosure of patient-specific information.

The Privacy legislation was designed to put additional autonomy in the hands of the patient who is receiving healthcare. It was to give the patient the control to decide who is able to access his or her healthcare information. Information protected under the privacy rulings is identified as Protected Health Information (PHI). The PHI includes such things as name, address, birth date, social security number, and similar personal information.

There are three main components within the privacy rule (Kennedy-Kassebaum, 1996): First, the rule gives flexibility to the healthcare entity to define whether they will obtain written consent from the patient before carrying out treatment, payment, or healthcare operations.

Second, the rule requires written or verbal authorization for use and disclosure of personal health information for purposes other than treatment, payment, or operations. The required authorization applies to both paper *and* electronic medical information. The authorization can be revoked at any time by the patient. The rule does not, however, apply to release of information to governmental officials for law enforcement, public health, and research purposes.

Third, the Administration Requirements state that an organization that receives patient identifiable information must meet the following five criteria: (a) designate a privacy official for their organization, (b) conduct a privacy training program for their employees, (c) implement verification procedures, (d) maintain policies and procedures for health information, and (e) give notice of privacy practices to the patient.

As stated above, the second component (authorization) requires written or verbal authorization for use and disclosure of personal health information for purposes other

than treatment, payment, or operations. More specifically, authorization consent must contain the following items: (a) a description of the information to be used or disclosed, (b) identification of the persons or class of persons authorized to make use of or disclosure of the PHI, (c) a description of use for each disclosure, (d) expiration date or event, and (e) the patient's signature and date. In addition, if the consent form is signed by a personal representative, a statement identifying authority to act on behalf of the individual must be included.

After signing the authorization, the individual has the right to obtain an accounting of any disclosures of their PHI made by a covered entity. The disclosure of PHI by a healthcare entity is to be "reasonable" within treatment settings. For instance, PHI can be shared between healthcare providers, bedside clinical documentation is allowed, and physician office sign-in sheets are generally considered reasonable.

The reasonableness of these standards, however, is likely to be debated by the industry and the consumer as privacy regulations continue to be implemented. Such debates are likely to include discussion about the release of personal information for research purposes and law enforcement (Kouzoukas, 2002).

Currently, authorization of PHI for research purposes enables healthcare entities to release PHI with written consent (which may be combined with the general consent form). The Privacy Rule and the Federal Policy for the Protection of Human Subjects (Common Rule §164.512) are now more consistent, since the Privacy Rule supports the Federal Policy for the Protection of Human Subjects rule (Kouzoukas, 2002).

Three components of the privacy rule relate directly to the Federal Policy for the Protection of Human Subjects. First, there are sections related to "minimal risk to

privacy” which include a plan to protect identifiers, a plan to destroy identifiers, and assurances against re-disclosure. Second, there are sections relating to the impracticability of the research without a waiver. And third, there are sections related to the impracticability of the research without access to the PHI.

De-identification of PHI from research activities is required. This is achieved by an expert opinion that there would be a small risk the PHI could be used to identify an individual. But researchers argue that de-identification of the PHI can impact the value of the research being collected. The challenge is to maintain a minimal set of PHI in order to maintain the value of the research, while at the same time limiting the ability of the PHI to be re-identified and used for unauthorized purposes.

Authorization for release of PHI to law enforcement is not required, nor is the authorization for release of PHI to public health officials required. Both of these entities are preempted by existing standards related to Center for Disease Control, Department of Health and Human Services, and Child and Adult Protective Services. Healthcare entities have already expressed concern about balancing patient authorization between what is accepted by the patient as reasonable disclosure and what may be perceived by the patient as unreasonable (Federal Registry 65, 2000, Comment Section).

Statement of the Problem

As healthcare entities continue to scramble to be HIPAA compliant, they must enforce policy changes that require patients to read, sign, and express understanding of the organization’s privacy policies. It appears, however, that the patient’s perspective on healthcare privacy has not been considered in either the formation or implementation of policies required by the HIPAA privacy component. Patients are healthcare consumers,

yet little research has been done on assessing the individual consumer's perspective on what Protected Health Information (PHI) is actually important to protect and from whom it is important to protect it.

Does the healthcare consumer really value the defined PHI? If so, what elements of the PHI are most valued? Does the healthcare consumer really want to control the accessibility of healthcare information to healthcare providers, insurance providers, researchers, law enforcement, and employers? If so, whose access to information does the healthcare consumer want to see limited, and to what degree? Also, how much personal economical backing does each PHI carry from the healthcare consumer's perspective?

These questions are addressed in this study. It is predicted that the current PHI as defined by HIPAA privacy regulation does not match the healthcare consumer's perspective of what information is important to protect, and from whom that information must be protected. It is also predicted that the healthcare consumer is not willing to pay more for healthcare services to protect their personal PHI.

Purpose of the Study

The purpose of this study was to survey a selected population of healthcare consumers (patients) to identify their perspectives on certain personal privacy issues related to the HIPAA PHI indicators. The study focused on four key areas: (a) the type of information the consumer wants to keep private; (b) the relationship of age, nationality, gender, and authority level in the desire for privacy; (c) who should access information; and (d) the economical priority given to protecting each PHI indicator.

More specifically, this study evaluated the perspective of those healthcare consumers (patients) who participate in the Carnegie Financial Insurance third-party

payer plans. The Carnegie Financial Insurance "Internet members list" was selected as the population to survey. Participants on the membership list were quantitatively surveyed for their perspective on the value of each PHI indicator. Their responses helped to indicate the degree to which healthcare consumers believe the protection of private information between various healthcare entities was desirable.

Data collected in this study will prove valuable since it will offer consumer-based reaction to current HIPAA PHI regulation. This could lead to more informed decisions when formulating future public policy, and to more efficient utilization of resources within the healthcare setting.

Research Questions

The purpose of the research questions was to identify whether healthcare consumers (patients) find the privacy of current HIPAA PHI indicators important, and to discover the degree to which they want PHI indicators protected by healthcare entities. Most individuals who grant authority to healthcare providers trust the reputation and competency of healthcare professionals. They are willing to be "transparent" and to allow their personal information to be in the hands of their healthcare providers (Louis Harris and Associates, 1993).

I have hypothesized that consumers prefer "Healthcare Transparency" —a concept centered around the idea of full information exposure in order to obtain the greater good (the gift of wellness). Healthcare Transparency, suggests a direct relationship between healthcare consumers' need for quality cost-effective care and their willingness to release personal healthcare information. The Healthcare Transparency model will be more fully developed in the theoretical section of this study.

In addition, the myriad of reimbursement structures within the healthcare industry means that protecting personal PHI has strong economic ramifications. I have further hypothesized that consumers of healthcare are not willing to pay more for healthcare services in order to keep their PHI “protected” from qualified healthcare professionals.

The theory of Healthcare Transparency gives rise to the following research questions:

1. What components of Protected Health Information (PHI) do patients want to keep confidential from their healthcare providers?
2. What is the relationship of demographic factors in the desire for privacy?
3. What is the relationship between authority ascribed to physicians’ and who has access to healthcare information?
4. What is the level of financial commitment given by the patient to protect each element of Protected Health Information (PHI) mandated by the HIPAA privacy rule?
5. What other information do respondents think should be kept private?

The response to the research questions will indicate whether healthcare consumers believe PHI indicators should be kept private from healthcare providers (Federal Register 67, 2002), and whether they are willing to pay to protect their personal PHI.

Theoretical Framework

The concept of “transparency” came to be recognized in the days of Pericles when citizens would gather at the Academy in Athens and openly debate issues of the day. Socrates was among the citizens who openly shared his views, and he openly criticized the democratic political leaders for their lack of wisdom and ability to govern with

virtue—a quality essential for rulers (Oliver, 1997). Socrates paid a high price for his open, transparent criticisms. The Athenian rulers executed him.

Plato, Socrates' devoted student, was burdened by Socrates' execution for his outspoken beliefs. He responded by writing about the "closing" of society. In *The Republic*, Plato (1968) stated that people's desires and talents must be contained for the good of the whole community. He stated that the freedoms presented by the concept of democracy are good in the short term, but wasteful in the long term, to society as a whole. A ruler must be able to manipulate the human resource in order to create the perfect society (Plato, 1968). Throughout the centuries, governments have relied on Plato's theories to justify ruling with tyranny (Brin, 1998). But the closing of society serves only to isolate the individual, protect tyrannists, and perpetuate injustice.

In more modern times, the open society theories of Pericles have been revisited and the academy of thought resurrected. Brin (1998) asserts that "free speech is seen as the best font of criticism, the only practical and effective antidote to error" (p. 326). When individuals speak out, exposing rights and wrongs, it brings justice and accountability. This is supported by a legal system for debating issues, a system that honors the "whole truth and nothing but the truth." Individuals with honor and integrity have little to fear in such a system as long as the road is a two-way street open to all.

Many believe that protection from tyrants who would oppress and conspire against transparent individuals is best found by building walls, by creating "private gardens" so that freedom is secure "within the mind" (Brin, 1998). Yet Brin points out the following:

This has been tried, and there is not a single example of a commonwealth based on that principle that thrived. There is a better way. . . . Accountability is a light that can

shine even on the gods of authority. Accountability is the only defense that ever protected free speech, in a garden that stands proudly, with no walls. (p. 327)

There have been many experiments in creating an open or transparent society. Jeremy Bentham (1787/1995), philosopher and social architect, developed the “panoptic” model of constant surveillance as a means to social control within institutions. The Panopticon is a ring-shaped structure with windows on all sides that face into the quarters of those being observed. This allows individuals to be under constant surveillance (Brin, 1998). Bentham created the idea as a means for controlling prisoner behavior. The concept is to provide an environment where an individual is aware of continuing surveillance day and night. The surveyed is aware that the “inspector” is always present. He sees the constant shadow of the inspector, and hears his voice when the inspector chooses to convey a message.

Whitaker (1999) suggests that Bentham drew a comparison between social observation and religion, between the Panopticon and an invisible, all-knowing God. Just as the inspector within the Panopticon cannot be seen, but can reveal at any time the violations committed by the observed, so an unseen God reveals his knowledge of mankind’s wrongs through Scripture, with the implication that consequences await.

Bentham’s underlying philosophy was that when an individual knows he is being observed, it changes his consciousness (Brin, 1998). Based on this idea, Whitaker (1999) suggests that transparent societies might be safer and better maintained. Michel Foucault (1979) has stated that Bentham's theory of social control through panoptic principles was a “mechanism of power reduced to its ideal form” (p. 205). He believed panoptic principles could be applied to social systems for the purpose of generalized *surveillance* rather than discipline. Foucault (1979) spoke of the formation of a disciplinary society

focused on “a sort of social quarantine” rather than “enclosed disciplines” (p. 216).

Foucault believed that infiltrating panoptic principles into the capitalist workplace was a good starting point (Whitaker, 1999). Whitaker supports this view, stating that “such knowledge is a productive resource, and nowhere has this been more evident than in the organization of the capitalist workplace” (p. 38).

Adam Smith (1776) planted the seeds for a panoptic economic system in an early manufacturing model. He described how a pin factory could be made more productive by segregating the tasks into different operations. Henry Ford and Frederick Taylor adapted this model to create a panoptic (transparent) system within the workplace, resulting in higher product yields and improved quality (Whitaker, 1999). Ford’s automotive assembly line supported Bentham’s theory of controlled behavior. Each assembly line worker was constantly surveyed and assessed by the next worker down the line. If a worker did not assemble a component properly, then it was immediately discovered and reported. If the negligent worker’s behavior did not improve, he was dismissed. This panoptic system created an incentive for monitoring other workers since failure by one worker made it impossible for the task to be completed. If one individual in the system was not accountable to the process, then all were unsuccessful.

According to Whitaker (1999), panoptic (transparent) ideals seem to work within the workplace because they are reciprocal. Workers are not only being monitored, but they are themselves serving as monitors. Whitaker suggests that applying panoptic principles to a capitalist society is necessary in order to maintain an economic advantage. Panoptic (transparent) concepts also relate to broader social structures. In *The Open*

Society and Its Enemies, Karl Popper (1962) wrote that during the Cold War, society was opening and becoming more transparent:

[People were] freeing themselves and their minds from the tutelage of authority and prejudice . . . their unwillingness to leave the entire responsibility for ruling the world to human or superhuman authority, and their willingness to share the burden of responsibility for avoiding suffering, and to work for its avoidance. (p. 23)

Popper (1962) believed that political power was the key to economic power, and that economic power must be controlled by political power in order to prevent exploitation. He used Marxism as an example of how economic power decapitated political power and therefore closed societies. Popper criticized Karl Marx for his inability to see the dangers of economic power. He felt Marx's view that a classless society would dissolve state power showed that Marx did not understand the needs of human freedom. He dismissed Marx's theories on the grounds that the "less gifted, less ruthless, or less lucky could become objects of exploitation" (p. 127). Instead, Popper believed that democracy was the only way citizens could protect themselves against misuse of political power, and the only way rulers could be controlled by the ruled. This control could be maintained through property rights, since the ability to gain and maintain property gives citizens an economic footing. Property is protected through legislation, legislation is maintained through social infrastructure, social infrastructure is maintained through taxation, and taxation is supported and maintained through transparency and an open society.

Writing in *The Right to Privacy*, Judith Jarvis-Thomson (1975) supports the view that privacy protection can be established and maintained through property rights as opposed to governmental mandates. She offers the following example:

To own a picture is to have a cluster of rights in respect to it. The cluster includes, for example, the right to sell it to whomever you like, the right to give it away, the right to tear it, the right to look at it. These rights are all 'positive rights': rights to do certain things to or in respect of the picture. To own a picture is also to have certain 'negative rights' in respect of it, that is, rights that others shall not sell it or give it away or tear it. (p. 298)

One's ability to control one's property independent of governmental intervention is a positive right. To be able to sell personal property or information, give it away, or keep it private is a right that should be controlled by the individual under the context and protection of property rights as defined by the Fourth Amendment.

Yet certain personal information about a society's citizens is vital to its infrastructure. To maintain infrastructure (schools, healthcare institutions, safe cities, etc.), citizens must be willing to pay taxes. In order to tax fairly, information (census) must be collected about the distribution of property and income. Additional personal information (statistics) provides society with a measuring stick to grade itself socially, economically, and culturally. Such information helps provide a kind of collective self-consciousness.

In order for social systems to survive and grow, a degree of transparency about personal information is critical. Compliance with this transparency becomes the key to economic, political, and cultural stability. Monitoring compliance and deviations from compliance allows a social system to reinforce its standards and maintain order. This reinforcement is then passed on to other social systems (schools, workforce, community). The benefit of the panoptic (transparent) approach can be surety of stability for education, income, public safety, and enjoyment.

David Brin (1998) refers to Perciles, Popper, Bentham, and Foucault in his views on transparency. However, Brin brings a more human touch to transparency. He believes

that "the flow of information is the flow of life" (p. 333). Transparency is not about forgoing privacy, but about giving society the power to hold accountable those who would violate privacy. Brin states that those who want to do harm have far more freedom to do so in a world of secrecy than in a world of light.

Secrecy can be dangerous. An elderly woman falls in her apartment and no one discovers her for days. A child is repeatedly abused and no one is aware of it for years. In a totally open society, these instances could not occur. Everyone would be constantly aware of those around them. Your financial information might be public, but so would any wrongdoing by a politician who misspent your taxes. Complete knowledge of other cultures could lead to increased tolerance of diversity. Healthcare service could improve as more funding was available for research instead of being spent on regulatory and administrative costs.

Esther Dyson (as quoted in Brin, 1998) stated, "The challenge is not to keep everything secret, but to limit misuse of information. That implies trust, and more information about how the information is used. At the same time we may all become tolerant if everyone's flaws are more visible" (p. 310).

Richard Wasserstrom (1984) suggested that not disclosing personal facts and details about oneself may not only be deceptive, but also morally wrong. He presumed that an individual feels humiliated or embarrassed because their ideas or actions are outside the norm. Secrecy prevents that individual from knowing that many others may have thought or acted in the same way. If the individual knew this, he would see himself as more "normal," and could be more willing to share information.

Ferdinand Schoeman (1984) states that "concern over one's own privacy may be regarded as a sign of moral cowardice, an excuse not to state clearly one's position and accept whatever unpopularity might ensue. Privacy may be seen as a culturally conditioned sensitivity" (p. 1).

Relinquishing private information has been identified in anthropological data as particular to enculturation (Gray-Lukkarila, 1997). Wasserstrom (1984) suggests the following:

Indeed our culture would be healthier and happier if we diminished substantially the kinds of actions that we now feel comfortable doing only in private, or the kind of thoughts we now feel comfortable disclosing only to those with whom we have special relationships. . . . There is simply no good reason why privacy is essential to these things [for example,] sexual intercourse could be just as pleasurable in public (if we grow up unashamed) as is eating a good dinner in a good restaurant. Sexual intercourse is better in private only because society has told us so. (p. 331)

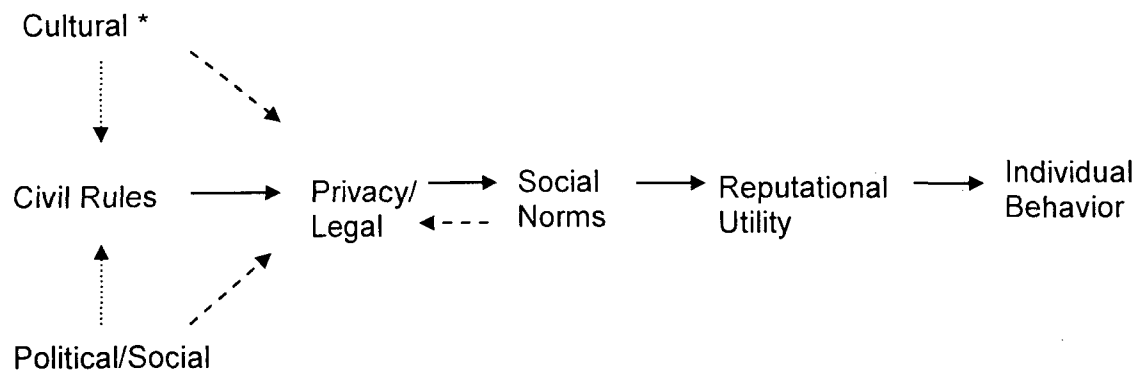
Wasserstrom (1984) states his beliefs further:

Privacy generally advocates concealment and deception. If individuals were more relaxed and at ease with who they were as private beings, their characters and dispositions would become more harmonized and they would come to feel less intimidated to represent themselves as other than they actually are. (as quoted in Gray-Lukkarila, 1997, p. 19)

There is ignorance over the fact that an individual's own condition is universal and is not an idiosyncratic aberration (Schoeman, 1984). In American culture, we tend to protect personal privacy in order to maintain our image of personal self (Gray-Lukkarila, 1997). Yet not divulging who we really are to those with whom we interact could be seen as deceitful.

Tal Yuval (1997) has defined how privacy and social norms have a causal connection to individual behavior. Figure 1 shows how individual behavior is governed by the reputational utility, which is impacted by social norms, which are regulated by

privacy mandates. The culture and political norms of a society help formulate privacy legislation, which in turn dictates social norms. These social norms define how a community is to live. Those who fall outside the social norm develop reputations for non-compliance. Often social norms dictate not only how individuals behave, but to what extent they are willing to release personal information and to whom.



*Cultural refers to a cultural norm with respect to privacy levels, rather than to culture in general and broken arrows mean that the causal connection portrayed does not always exist.

Figure 1. Causal connection between privacy, social norms, and individuals' behavior.

A free society that desires to grow economically, to provide for its members' freedom of knowledge, and to produce happy members with a positive well-being, is best served through an open, transparent society that values personal accountability. In other words, "an individual's right to privacy could be sacrificed in order to preserve the well-being of the community" (Gray-Lukkarila, 1997, p. 5).

The tyrants who would oppress and conspire against transparent individuals are ever present. In current society, the only antidote to protect individual freedoms appears

to be regulatory controls mandated by the government. Regulations tend to support the construction of private sanctuaries for individuals to live within—thus protecting them from harm. But Schoeman (1984) states a different view:

The right to privacy is seen as creating the context in which both deceit and hypocrisy may flourish; it provides the cover under which most human wrongdoing takes place, and then it protects the guilty from taking responsibility for their transgressions once committed. (p. 1)

A person who enjoys privacy is said to have the ability to control whom they choose to release information to, and to whom they choose to keep information from (Fried, 1968). Yet to mandate who can give and receive information supports the concept of private sanctuaries that hold and restrict the individual.

Accountability—both personal and professional—is an option to private sanctuaries. Accountability has no boundaries; it is ever present to all. According to Brin (1998), “accountability is the only defense that ever protected free speech, in a garden that stands proudly, with no walls” (p. 327).

The accountability brought about by social transparency may be necessary for individuals to thrive socially, economically, and politically. Notice the words of Peter Schwartz and Peter Leyden (1997), commentators of the magazine *Wired*:

With the coming of *Wired*, global society, the concept of openness has never been more important. It's the linchpin that will make the new world work, in a nutshell; the key formula for the coming age is this: Open, good. Closed, bad. Tattoo it on your forehead. Apply it to technology standards, to business strategies, to philosophies of life. It's the winning concept for individuals, for nations, for the global community in years ahead. (p. 15)

Societies based on secret private gardens tend to turn inward, fracturing themselves into pieces. This nourishes rigidity of thought, inhibits economic growth, and increases poverty, mutual fear, and intolerance (Brin, 1998). By contrast, open,

transparent societies turn cultures outward, causing them to be receptive to new truths and new ideas, global tolerance and trust, fair trade, smaller more efficient economic units, and a virtuous world (Brin, 1998).

Healthcare Transparency

The opposite of controlling information is to relinquish it. David Brin (1998) illustrates the point:

Telling a physician what they may or may not know about a patient's health . . . may be effective for a little while, but soon you could find yourself embarked down a dangerous river, one whose *reductio ad absurdum* terminus is hell. (p. 81)

In an emancipated (decentralized) society, it is essential to social order that individuals are willing to trust and exchange information with complete strangers. Brin (1998) argues that we are all members of a civilization:

Openness and candor are essential for the survival of any civilization, especially a global throng of over six billion human beings. Many aspects of openness are already so deeply rooted in the system that nothing will ever tear them out. At least, not without surgery so brutal that it would take the annihilation of millions. (p. 144)

Historically the American healthcare industry has constructed a culturally, politically, and socially open infrastructure based on the reputation of healthcare professionals to keep information private. This information is used to render care, conduct research to improve health, provide payment for services rendered, and to protect society (protection from epidemics, etc.). Healthcare Transparency simply continues the same principles of openness as a way of increasing economic stability, expanding the knowledge base through clinical research, and bringing about the efficiency of healthcare delivery that will ultimately improve human well-being and provide the greatest good for the greatest number.

Mel Thompson (1994) says this in his book, *Ethics*:

Society is complex; it does not consist of uniform people, all wanting the same things, or expressing the same preferences. There will always be conflict of interests and divergences of views. Now utilitarianism has taken this into account to a certain extent by allowing for 'preferences' to be expressed, rather than imposing on others what we consider to be best for their greatest happiness. Nevertheless, the final decision is made in the interests of the majority. (p. 102)

In healthcare, the greatest happiness for the greatest number means providing continued quality healthcare at cost-effective prices. Healthcare Transparency can be a significant tool in achieving this goal.

Machiavelli held that "less harm will be done by decisive action than by a compassionate but indecisive muddle" (quoted in Thompson, 1994, p. 119). Protecting individual privacy and supporting transparency is a trade-off; the protection of individual privacy gets exchanged for various personal and societal goods (Smith, 1994).

J. Smith (1994) asks a key question: "How do corporate executives and employees perceive privacy concerns?" (p. 155). The healthcare executives whom he surveyed identified that "a certain use of information might result in 'a little loss of privacy' or a 'slight intrusion'" (p. 156). Smith quotes a "LifeIns" executive:

Sometimes, you just have to do what is right, even if it loses business. That's happened to us several times in deciding on releases of AIDS test information and in dealing with disclosures to agents. We know the underwriting statistics, and we know what death rates will be. So, I can make decisions about what to do with information just because they're the right decisions. If we lose a little business in some particular situations, so what? We won't starve. (p. 157)

The splinter group of consumers within J. Smith's (1994) study responded that "total disclosure in society would be a good thing, since only guilty people need to worry about privacy" (p. 157).

Since the current healthcare market is a myriad of social, political, and cultural structures, all of which have been put in place to meet consumer demand for quality healthcare, the idea of Healthcare Transparency within healthcare promises to be both interesting and threatening.

Risk Adverse

Since risk is defined as the possibility of loss or injury (*Merriam-Webster Online*, 2004), an individual's willingness to release personal information is directly proportionate to the level of perceived risk. In other words, individuals will assume greater risk if they are in control of a situation than if they are not. Yet when individuals feel a loss of control, but still want to achieve a desired outcome, they are more willing to place their trust in strangers and to trade personal information for personal convenience (Brin, 1998).

The healthcare industry relies on this willingness to exchange information with strangers. Individuals trust and release information to healthcare "strangers" because they perceive that the risks involved in *not* giving information are greater than the potential risk of information reaching an inappropriate source. Their primary self-interest is in getting needed medical attention, and this means sharing daily practices and intimate secrets in order to assist the provider in coming up with an accurate diagnosis. From the perspective of risk, protection of private information from healthcare entities may be neither desired nor needed. The theory of Healthcare Transparency, the willingness of the healthcare consumer to be transparent with personal information in order to achieve the greatest good, will be explored in this study.

Significance of the Study

The study will seek to identify what elements of the Protected Health Information (PHI) healthcare consumers (patients) want to protect and from whom. This knowledge could lead to more defined public policy and more efficient utilization of resources within the healthcare setting.

It is predicted that the defined HIPAA PHI information the healthcare consumer wants to keep confidential is very limited, and is not all covered by the defined HIPAA privacy regulation. Age is predicted to be a factor in considering the type of information that is desirable to protect. Healthcare consumers who grant full authority to their physician for their healthcare decisions are predicted to also grant full access to their healthcare information. Nationality is not predicted to play a factor in what health information is considered desirable to protect. It is also predicted that the financial commitment of healthcare consumers to protecting each PHI will be limited.

Procedures needed to implement authorization and track PHI data that have been released will be extremely costly to America's healthcare entities. The costs of the privacy component of the HIPAA regulations are estimated to exceed even the Y2K expenses of \$8.3 billion (HIPAA Advisory Board, 2001).

A Nolan Company analysis determined in 2001 that over the course of 5 years the healthcare industry would need to spend \$42.9 billion in order to become HIPAA compliant (Hofmann, 2001). The Nolan Company recognized that the Administrative Simplifications components of HIPAA may save the federal government about \$29.9 billion over 10 years—but the government neglected to include the costs to healthcare

organizations for improving information system technologies and other infrastructure needs in order to meet HIPAA requirements (Hofmann, 2001).

Estimates of complying with the privacy component of the HIPAA regulations can be broken down as follows: \$4 billion for inspecting and changing records, \$9 billion for tracking of disclosed information, \$23 billion infrastructure cost such as retraining staff and hiring privacy officers, \$3 billion in added medical cost from reduced medical management, and \$4 billion for monitoring “business partners” (Blue Cross/Blue Shield, 2002)—for a total of approximately \$43 billion.

Healthcare privacy within HIPAA regulations carries significant challenges, not only in costs and implementation, but also because it is a “major shift in the way we do healthcare” (Lemov, 2002, p. 46). According to Richard Varn (quoted in Lemov, 2002), “HIPAA is the biggest upgrade of healthcare technology in the U.S. since we discovered bacteria” (p. 46).

Compliance for the privacy regulation was set for 2003 and each healthcare entity was required to meet the obligation of protecting all the elements as defined in the rules for Protected Health Information (PHI). Those elements identified as “protected” were defined at the federal level. Consumer (patient) input as to the importance of protecting the PHI from various healthcare entities has been minimal, and no degree of the importance of each PHI has been identified.

Identifying the answers to the research questions will assist in providing consumer input and information related to the HIPAA privacy regulation. Additional information can help with redefining public policy related to healthcare.

Restructuring public policy—explicitly public policy dealing with privacy of personal information—is a complex endeavor that requires knowledge of the human spirit and the principal values held by each individual and the society in which the individual resides. Privacy is not a constitutional right, nor is it a law. Rather, it is a philosophy that has been embraced by the human spirit and claimed as a human right.

Definition of Terms

The following terms are defined as used within this study:

Department of Health and Human Services (DHHS): The United States government's principal agency for protecting the health of all Americans and providing essential human services, especially for those who are least able to help themselves (Bureau of Primary Healthcare, 2000).

Protected Health Information (PHI): The privacy provisions of the federal law, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), apply to health information created or maintained by healthcare providers who engage in certain electronic transactions, health plans, and healthcare clearinghouses. The Department of Health and Human Services (DHHS) has issued the regulation, "Standards for Privacy of Individually Identifiable Health Information," applicable to entities covered by HIPAA (Privacy Rule, 2002).

Health Insurance Portability and Accountability Act (HIPAA): The Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II) require the Department of Health and Human Services to establish national standards for electronic healthcare transactions and national identifiers for providers, health plans, and employers. It also addresses the

security and privacy of health data. Adopting these standards will improve the efficiency and effectiveness of the nation's healthcare system by encouraging the widespread use of electronic data interchange in healthcare (Kennedy-Kassebaum, 1996).

Healthcare Entity: A particular healthcare institution, such as an acute care hospital, nursing home, or nursing facility (Pozgar, 1996).

Healthcare Provider: A particular healthcare institution or individual that provides personal care services to the patient population (Privacy Rule, 2002).

Gross National Product (GNP): The GNP of a country is the total amount of goods and services produced by the labor and capital supplied by the country, regardless of whether it is located within the borders of the country (Organization of Economic Development, 1991).

Third-Party Payer: Payer of services, outside the individual who is receiving the service, such as an insurance company (Kennedy-Kassebaum, 1996).

Transparency: Free from pretense or deceit, easily detected or seen through, or readily understood. Synonyms include, clear, frank and obvious (*Merriam-Webster*, 2004). In humanities, transparency implies openness, communication, and accountability. It is a metaphorical extension of the meaning used in physical science: a transparent object is one that can be seen through (Wikipedia, 2007).

Privacy: Withdrawn from company or observation, not known or intended to be known publicly, preferring to keep personal affairs to oneself (*Merriam-Webster*, 2004).

Delimitations of the Study

It is recognized that the current study poses some delimitations and therefore limits the external validity of the research findings:

1. The survey results are limited to the Carnegie Financial Insurance "Internet list group."
2. The survey was distributed electronically. Therefore individuals who do not utilize a computer are not represented in the survey results.
3. The survey results are limited to those individuals who carry third-party payer coverage. Therefore individuals who are uninsured may not be represented in the study findings.
4. Individuals who are unemployed may not be represented in the study findings.
5. Elderly or poor healthcare consumers who carry medical coverage through Medicare and/or Medicaid may not be represented in the study findings.

Organization of the Study

The organization of the study includes the abstract, which outlines the overview of the research study. Chapter 1 contains the introduction and statement of the problem, purpose of the research, significance of the study, theoretical foundation, definition of terms, and delimitations of the study. Chapter 2 presents a review of the literature, with sections outlined as Origin of Privacy, Key Judicial Cases and Legislation Related to Privacy, Healthcare and Privacy, and Transparency. Chapter 3 presents the research methodology including the limitations of the study. Chapter 4 presents the findings of the research study, and chapter 5 summarizes the entire study and presents the conclusions and recommendations for further study. The appendix and the reference list can be found at the end of the study.

CHAPTER TWO

LITERATURE REVIEW

The purpose of this study was to survey a selected population of healthcare consumers (patients) to identify their perspectives on certain personal privacy issues related to the HIPAA (Health Insurance Portability Accountability Act) privacy rule. The study focused on the type of information the consumer wants to keep private; the relationship of age, nationality, gender, and authority level in the desire for privacy; who should access information; and the economical priority given to protecting each PHI indicator.

Literature review strategies used in this study include electronic literature searches using *Dissertation Abstracts International*, FirstSearch, Ovid, CINAHL, MEDLINE, and LEXIS-NEXIS. The terms used in the computer searches were “privacy,” “issues,” “ethics,” “healthcare,” “HIPAA,” and “transparency.”

Little research was found that directly pertained to the patient’s perspective of the HIPAA Protected Health Information. Available privacy literature is primarily centered on case law, organizational compliance, Internet privacy, and financial privacy.

Since results on research on the subject of privacy and transparency varied, the selection of pertinent studies was limited to those researchers who have a cross section between privacy and transparency. There were also a number of key judicial cases that specifically dealt with privacy concerns. Scholars and judicial cases setting precedence

for understanding privacy, as well as current research on privacy and transparency, will be addressed within the following pages.

The literature review is divided into three key areas: First, the origin of privacy as related to culture, personal identity, and scientific evolution; second, key judicial cases supporting the concept of privacy within society; and third, the transparent side of privacy issues, and the discrepancies that exist between expressed privacy concerns and individual responses to procuring privacy within society.

Origin of Privacy

The concept of privacy evolves from a sense of self (Hendersen, 1999). It grows from an understanding that there are some things uniquely personal and within, and others that are global and outside of the self. It involves realizing that these things may or may not pose a threat if known. Understanding these cultural and psychological roots helps put the origins of privacy in context.

During the Middle Ages (and in many tribal societies today), privacy was not well known. Privacy may have been desired, but it was not readily supported. Many people lived together under one roof, each observing the personal attributes of the others. Members of tribal communities saw anger, despair, sexual behavior, and many other forms of expression between family members that we now consider private.

In 1215, the British Magna Carta was implemented by King John of England. Before this time, rights of personal freedom had been directly connected to social status. Those who possessed land or found favor with rulers were considered more powerful than others, and possessed certain rights. Those who did not have social status were considered dispensable, and their persons and possessions held no rights. The Magna

Carta gave the common people of England rights previously unknown. It set controls over imprisonment (habeas corpus). It gave merchants the right to come and go. It allowed people to freely choose a church. It allowed them to avoid unfair taxation (Duhaime Law Museum, 2002). The Magna Carta not only gave the British people the foundation for more protection for their possessions, but also more autonomy within their lives, which produced a sense of self-awareness and the desire to protect one's existence.

Concepts of personal property and privacy continued to grow throughout the Renaissance period. Personal emotions and feelings began to be transcribed into written words through poetry and other literary works. As journals and diaries became popular, one's personal thoughts were hidden under lock and key (Fowler, 1987). Self-expression was also displayed in dramatic arts and sonnets that explored personal emotions and gave great importance to personal identity (Fowler, 1987). Miller (1971) refers to the following excerpt from William Shakespeare's *Othello* to introduce the idea that specific personal information can also be a kind of property:

Who steals my purse, steals trash: 'tis something, nothing;
'Twas mine, 'tis his, and has been slave to thousands:
But he that filches from me my good name
Robs me of that which not enriches him,
And makes me poor indeed. (Act III, Scene iii)

In other words, if the information which influences a person's reputation is taken away, then a valuable form of property has been stolen. This gave focus to the concept of the value of identity and the uniqueness of each individual.

In the decades following the Renaissance, four key philosophers influenced the political thinking on individual privacy rights: Thomas Hobbes, John Locke, Jean-Jacques Rousseau, and John Stuart Mill.

Thomas Hobbes (1651) stated that there is no truth, reason, or justice in human nature and that man lives in a constant state of fear and danger. Hobbes felt man must either live with the instinctual egotistical foundations of human nature, or give way to a government of absolute power that could offer harmony and comfort. Hobbes supported strong governmental controls to restrict personal autonomy, thereby building a foundation of political infrastructure that could put requirements on society to live in a certain way.

John Locke (1690) believed people by nature had a right to liberty (political equality), life, and ownership of property. He described this in his *Two Treatises on Government*:

Men being, as has been said, by nature all free, equal, and independent, no one can be put out of this estate and subjected to the political power of another without his own consent, which is done by agreeing with other men, to join and unite into a community for their comfortable, safe, and peaceable living, one amongst another, in a secure enjoyment of their properties, and a greater security against any that are not of it. (p. 95)

But unlike Hobbes, Locke viewed men as having the natural ability to form contracts with each other, therefore creating a moral law. Locke refuted Hobbes's belief that the only way to bring harmony and comfort to mankind was through an ultimate authority. Instead Locke defined the ideal relationship between a state and its citizens as a contractual one—a constitutional government with a clear separation of powers between the legislative, the executive, and judiciary branches. The writers of the American Constitution were greatly influenced by John Locke (Oliver, 1997).

Jean-Jacques Rousseau was the first philosopher of the 18th century to question the bracketing of moral and political ideas (Oliver, 1997). Rousseau is best known for his romantic style of thought. He believed that man's natural state combined a communal life

with passionate egoism. In *The Social Contract* (1762), Rousseau wrote, "Man was born free, and he is everywhere in chains" (p. 1). His social contract theory states that the legitimacy of the state is based on the agreement of individual human beings to surrender some or all of their private rights in order to secure the protection and stability of an effective social organization or government.

John Stuart Mill (1859) explored the "Greatest Happiness Principle" in his essay *On Liberty*. He held that "actions are right in proportion as they tend to promote happiness, wrong as they tend to produce the reverse of happiness" (p. 14). Mill also pointed out that there is a relationship between the part of a person's life that seems to concern only himself, and that which concerns others. He believed the two could not be separated since the conduct of one member of society influences and impacts other members of society. If an individual causes harm to himself, his actions affect at least his near connections, and often others far beyond them. Mill spoke of property and its relationship to societal impact:

If a person injures his property, he does harm to those who directly or indirectly derived support from it, and usually diminishes, by a greater or less amount, the general resources of the community. If he deteriorates his bodily or mental faculties, he not only brings evil upon all who depended on him for any portion of their happiness, but disqualifies himself for rendering the services which he owes to his fellow-creatures generally; perhaps becomes a burden on their affection or benevolence; and if such conduct were very frequent, hardly any offence that is committed would detract more from the general sum of good. Finally, if by his vices or follies a person does no direct harm to others, he is nevertheless (it may be said) injurious by his example; and ought to be compelled to control himself, for the sake of those whom the sight or knowledge of his conduct might corrupt or mislead. (p. 114)

Mill supported individual and social accountability, believing that no individual lives in isolation unto himself. Instead there is an ongoing obligation to one's community for the mutual good.

In review, Hobbes (1651) theorized that the deployment of absolute power brings peace, social controls, and protection of one's property; Locke (1690) supported balance of powers to bring equality between powers and individuals; Rousseau (1762) theorized the surrendering of rights for exchange of protection and stability; and Mill (1859) hypothesized personal accountability to society, where the conduct of one impacts all. Thus these four philosophers helped form public opinion on property rights and privacy.

America's founding fathers also understood that one's personal possessions could impact status and social ranking. They recognized society's desire to define and protect personal property. In 1791, the Bill of Rights guaranteed that one's possessions were protected against unlawful violation of intrusion by the government (U.S. CONST. amend. IV).

However, the Constitution took no direct stand regarding privacy between individuals. In America's early years, people were simply judged on the reputation they carried with them (Nock, 1993). Other than church documents, which recorded births, deaths, and marriages, there were very few written records.

Then in the 19th century, America experienced rapid growth through immigration. Many of these foreign immigrants settled in small communities. As these communities were flooded with strangers, the need arose for more substantial proof of reputation. One group that met this need was the Masons, a prestigious sect of individuals with an irrefutable reputation for integrity and financial accountability. A Mason who wanted to exchange goods or services simply presented a lapel pin, which signified he was of standing citizenship and could be trusted to bring forth his side of any bargain (Nock, 1993).

Commerce continued to grow in America and the industrial revolution emerged. More literacy was afforded to the general population. Utilization of the printing press, photographic images, and telegraphy added to the education of the American public. People began to trust the printed word, and information was now being disseminated at a rapid rate.

The Victorian era brought formalities to interactions between individuals and privacy etiquette was established. Social standards were refined, social rules for visitation, length of stay, and mixed company etiquette. Women were not considered prudent if they were out with a man unescorted. Visitors to a proper Victorian home were expected to be invited, and then upon arrival escorted to a waiting room until the “master” of the house would welcome them further into the private quarters of the home. Visits were recorded in the local newspaper, and news of people’s affairs spread through gossip channels. Through their prudent lifestyle, Victorians showed the value of privacy, and they embraced the idea of protecting that privacy within every aspect of their lives (Miller, 1971).

In 1876, Alexander Graham Bell introduced the telephone. People began to discuss private matters over the phone lines. Private matters were no longer exclusively contained in living rooms, offices, and street corners. The use of party lines and operator-assisted conversations allowed others to hear these private conversations. Some private conversations were even transcribed and publicized.

Publicizing of private affairs continued to escalate until it became a concern. In 1880, Judge Thomas Cooley expressed the idea that each of us has “the right to be let alone.” This was followed a few years later by the now famous 1890 *Harvard Law*

Review article, "The Right to Privacy," which defined the need for tort action for the "invasion of privacy" between private individuals and the press (Warren & Brandeis, 1890). Part of Samuel Warren's incentive for writing the article was the detailed publication of his wife's social affairs in the local paper. In their article, Warren and Brandeis outlined how photographs and mass circulation newspapers presented a threat to individual privacy. They claimed that personal reputation was no longer judged on known facts or social conversation, but gossip marketed and put on the printed page with pictures for all to see. Their writings laid the foundation for changes in the area of privacy law.

As the general public became more concerned about protecting their individuality in a greatly expanding culture, new discoveries were also being made in science and psychology. These discoveries seemed to undermine individual uniqueness and the importance of the inner self. Darwin's theory of evolution suggested to some that human beings were not unique and therefore open to evaluation (Hendersen, 1999). Karl Marx claimed that it was history that made people, not people who made history (Hendersen, 1999). Sigmund Freud (1911) stated that there were unconscious forces in the human mind that determined human behavior. Freud's use of dream interpretation and analysis of memories and feelings taught individuals to associate current conditions to past experiences. Not surprisingly, one reaction to these views was a new emphasis on privacy, especially the desire to protect the secrecy of one's personal health information.

Throughout the 20th century, the courts increasingly dealt with cases related to personal liberties and privacy rights. Questions were raised about how much the United States Constitution supported the right to individual privacy. Topics related to drugs,

sexual freedoms, incest, pregnancy, marriage, divorce, homosexuality, and computer technology were all brought before the courts. The concept of privacy became a debated issue with varying interpretations.

Richard Prosser (1960), a noted legal scholar, accumulated privacy cases and composed a prestigious essay known as "Invasion of Privacy." This court-recognized essay contained four torts addressing privacy issues from relevant cases. The four torts were as follows: (a) intrusion upon the plaintiff's seclusion or solitude or into his private affairs, (b) public disclosure of embarrassing private facts about the plaintiff, (c) publicity placing the plaintiff in a false light in the public eye, and (d) appropriation (for the defendant's advantage) of the plaintiff's name or likeness (p. 389). In practical terms, Prosser's scholarly work separated privacy concerns into four basic freedoms: the freedom to be "let alone" (as in Warren and Brandeis), freedom from public embarrassment, freedom from libel or slander; and freedom from one's name being used to benefit another.

Westin (1967) stated that a primary reason for seeking privacy is the desire to be insulated from observation. He suggests this is intimately related to certain motives such as avoiding criticism, punishment, or the discomfort of feeling inhibited. Westin also observed that "the legitimacy of group interests historically preceded the claims of individual interests" (p. 9). The question to ask is, "Does the 'greater good' (be it to society or the individual) outweigh the desire for privacy?"

Utilitarianism (as discussed by John Stuart Mill) is based on the concept that the good of the many outweighs the good of the few (Mill, 1859). He suggested that

sacrificing the privacy for those who have violated the "Greatest Happiness Principle" is warranted since the individual has caused more harm than good.

Privacy should not be viewed in isolation from other preferences of society. When privacy concerns conflict with other values that people hold, for example, economic well-being, then it is likely that privacy concern will give way (Gray-Lukkarila, 1997).

McClellan (1964) stated, "If people have to make choices, probably most Americans would rather give up some or much of privacy in order to gain what to them is the greater goal" (p. 40).

Roberts's (1993) focus on the personhood of privacy as privacy is not a "what" but a "who," a way of being whole. Roberts says, "It is a modern value that is explainable, in part, by the absence of the purely public with its resultant distancing of the individual citizens from participatory self governance" (p. 243). It is a "web" of interconnected conceptions—privacy, individuality, intimacy, and personhood; Roberts did not believe it was possible to separate these interests one from the other. Roberts recognized the importance of privacy but did not maintain that privacy was "more important than participation in the public, political or social realms for full development" (p. 245).

The delineation between what is private and what is public with the technological developments and globalization appear to be changing. "Weblogs," introduced in 1998, provide a place where individuals can post their thoughts, commentaries, essays, observations, and ideas. Commonly known as "blogs," weblogs have opened up the world to transparency of information. In today's technological, global society, information is deliberately shared, calling into question the relevance of Warren and

Brandeis's "Right to Privacy" writings about the once-coveted information of who you know and who you visit. The usage of "Face Book," an Internet tool for posting pictures, personal information about oneself, and listing all connected relationships, builds a web of interconnections between individuals. This web grows as more people assign themselves to each other. The information is available to all who wish to view it. The transparency—willingness to share one's associations, pictures, and personal information with others—appears to be a growing practice.

Meeler (2000) states that the last century concerned itself with privacy protection against unwanted publication of personal information but "sought generally to protect the products of the processes of the mind" (p. 11).

Transparency can benefit both society and those who want the safety and security. As of this writing, trial programs for other types of transparent systems are currently underway. A Florida husband and wife and their 14-year-old son have each been implanted with a computer chip called "Verichip." The tiny chip contains personal information about each family member corresponding to medical information kept in a database. Verichip's maker, Applied Digital Solutions, is promoting the idea that their product is ideal for situations where there is a medical emergency involving a person who is unconscious or mentally impaired. Their chip could provide an accurate medical history to doctors or nurses at the very moment it could matter most. Applied Digital Solutions also is testing the "Digital Angel" which uses GPS-style tracking to follow people's movements. Digital Angel is already being used in a pilot program to track Los Angeles parolees (Hilden, 2002).

The origin of privacy and society's practice of privacy rights has migrated from the desire to procure privacy from unwanted intrusion to willfully allowing exposure by conscious consent through willful participation. Legislation has followed suit with the migration of the views on privacy, as in protection of personal rights in the Fourth Amendment, which protects against unlawful search and seizure by the government, to the more socially transparent legislation such as the Wetterling Act of 1994, which protects citizens against harm to personhood and procures safer societies.

Key Privacy Legislation

In order to understand how privacy has come to be a valued and protected entity within our culture, it is important to understand the transition of privacy thought within our legislative and judicial systems. However, a full explanation of privacy legislation is beyond the scope of this study. Only key judicial reviews that pertain to the intent of this study will be listed. The key judicial cases discussed will be divided into three sections: (a) Key Judicial Cases and Legislation Related to Privacy, (b) Notable Supreme Court Cases Related to Privacy, and (c) Healthcare and Privacy.

Key Judicial Cases and Legislation Related to Privacy

Pamela Gray-Lukkarila's (1997) dissertation, *The Right to Privacy: Constitutional and Theoretical Foundations*, provides a comprehensive review of the constitutional framework for privacy. Gray-Lukkarila outlines how certain key judicial cases support the concept of privacy:

1. *Meyer v. Nebraska* (1923) established "zones of privacy" from governmental regulations (Gray-Lukkarila, 1997, p. 122).

2. *Pierce v. Society of Sisters* (1925) reflected Brandeis's work on intellectual privacy and parental liberties (Gray-Lukkarila, 1997, p. 123).

3. *Olmstead v. United States* (1928) is based on Brandeis's work with the concept of privacy and the right to be let alone (Gray-Lukkarila, 1997, p. 116).

4. *Griswold v. Connecticut* (1965) deals with the right of sexual privacy (Gray-Lukkarila, 1997, p. 125).

5. *Roe v. Wade* (1973) deals with abortion rights and the right to privacy (Gray-Lukkarila, 1997, p. 140).

6. *Bowers v. Hardwick* (1986) deals with sodomy law and the protection of privacy between two consenting adults to engage in sexual activity (Gray-Lukkarila, 1997, p. 149).

The expansion of social demands for the recognition of privacy grew out of ongoing social, political, and economic changes. In the 19th century, protection was only given for interference with life and physical property. The publication of "The Right to Privacy" (Warren & Brandeis, 1890) resulted in public recognition of the right to have a private life. Warren and Brandeis realized earlier protections were limited to protection from battery and the right to secure property. Their privacy tort expanded the term "property" to encompass every form of possession, intangible as well as tangible.

The first case to use their scholarly work took place in New York in 1902. A Miss Roberson sued a local milling company for using her picture to sell flour. Although the courts were conservative and rejected her plea to recover damages for "humiliation," the New York court concluded it is both a crime and a civil wrong to use anyone's name or

picture for purposes of advertising for trade without their permission (*Roberson v. Rochester Folding Box Company*, 1902).

In 1905, the Supreme Court of Georgia became the first court to recognize what is now referred to as “right to privacy” when Paolo Pavesich sued an insurance company for using his picture in a life insurance advertisement (*Pavesich v. New England Life Insurance Co.*, 1905). The advertisement depicted Pavesich as a sickly character who regretted not purchasing life insurance. Pavesich held that the insurance company violated his privacy rights by using his picture and implying he was worse off by not buying life insurance.

The Roberson and Pavesich cases established the foundation for litigating future privacy cases. Today, courts continue to use “right of privacy” as defined by Warren and Brandeis to describe a constitutional right to privacy (Gray-Lukkarila, 1997; Miller, 1971).

It should be noted, however, that given the impression of “a reasonable expectation of privacy” (Brin, 1998) at the state level, privacy laws do not apply to many behaviors related to individuals, corporations, or the press. Indeed, the courts continue to limit the “privacy expectations” of its citizens when dealing with such areas as law enforcement, observations by others for wrongful acts, telephone records, trash, and banking records.

Although the United States Constitution does not mention the word “privacy,” certain privacy rights are implied in the Bill of Rights (1791) and other amendments that followed the Bill of Rights. Sections of the Bill of Rights that pertain to privacy include the First Amendment (freedom of religion and expression), the Fourth Amendment

(freedom of unreasonable search and seizure), the Fifth Amendment (no legal duty to incriminate oneself), and the Ninth Amendment (implied rights not enumerated). Beyond the Bill of Rights, the Fourteenth Amendment also implies privacy rights (rights regarding life, liberty, or property). The Fourth, Fifth, and Fourteenth Amendments have particular relevance to privacy (Murphy, 1995).

The Fourth Amendment implies that persons, houses, papers, and effects are considered “private” possessions and should be respected as “secure”:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. (U.S. CONST. amend. IV)

In 1866, the Fourteenth Amendment extended the Bill of Rights from the Federal to the State level. Court rulings regarding the “papers, and effects” clause of the Fourth Amendment subsequently gave individuals much more control over their personal information. The safeguarding of privacy initiatives within the legislative body is now centered on the premise that personal information is a type of property (Miller, 1971). Thus, if an individual has the right to control their property against unlawful search or seizure, they then are also eligible for the full range of protection the legal system can offer as it pertains to the protection of personal information (Miller, 1971).

Richard Posner (1978) distinguished between two types of protected personal information: “discrediting” information and “embarrassing” information. Yuval (1997) later stated in his article on privacy and social norms that the latter point on “embarrassing” information often receives more privacy focus within our legislative structures than the first.

The Fourteenth Amendment also contains the “Due Process” clause, which mandates that the state may not “deprive any person of life, liberty, or property, without due process of law” (U.S. CONST. amend. XIV, §1). Due process is a legal concept ensuring the government will protect a person’s legal rights when the government deprives a person of life, liberty, and property. It places limitations on laws and legal proceedings in order to guarantee fairness, justice, and liberty (Wikipedia, 2006).

Gray-Lukkarila (1997) summarizes a 1973 discussion by Senator Sam J. Ervin, Jr., that supports this concept:

The First Amendment was designed to protect the sanctity of the individual’s private thoughts and beliefs. It protects the rights to speak and remain silent, to receive and impart information and ideas and associate in private and in public with others of like mind. After all, it is only by protecting this inner privacy that freedom of speech, religion, assembly, and many other individual liberties can be protected. The Third Amendment protects the privacy of the individual’s living space. This aspect of privacy is also protected by the Fourth Amendment’s guarantee of the “the right of the people to be secure in their persons; houses, papers, and effects, against unreasonable searches and seizures.” In addition to the privacy of his person (or bodily integrity), even his private telephone conversations are protected from unwarranted government intrusion. The Fifth Amendment guarantees that an individual accused of a crime shall not be forced to divulge private information that might incriminate him. This privilege against self-incrimination focuses directly on the sanctity of the individual human personality and the right of each individual to keep private information that might place his life and freedom in jeopardy. In *Roe v. Wade*, the Supreme Court has located the right of privacy in the Fourteenth Amendment’s guarantee that no state shall “deprive any person of life, liberty, or property without due process of law.” Rights to give and receive information, to family life and child rearing according to one’s conscience, to marriage, to procreation, to contraception, and to abortion are all aspects of individual privacy which the courts have similarly held to be constitutionally protected. (Gray-Lukkarila, 1997, p. 158)

Notable Supreme Court Cases Related to Privacy

The legal contribution to privacy as it relates to this study has been made with notable Supreme Court cases such as *N.A.A.C.P. v. Alabama*, *Griswold v. Connecticut*, *Katz v. United States*, *Bowers v. Hardwick*, and *Roe v. Wade*.

The case of *N.A.A.C.P. v. Alabama* (1958) provided a legal basis supporting the concept that an individual's name is a protected property. The N.A.A.C.P., a not-for-profit organization for the advancement of Negroes, opened an office in Alabama without complying with a state statute requiring a foreign (out of state) corporation to file its corporate charter, including its full membership list. In a landmark decision, the court stated that it was unlawful to require a not-for-profit organization to submit its membership list in order to conduct not-for-profit activities within the state. The court ruled that this list of names was protected as private information, and was to be controlled by the not-for-profit organization (*N.A.A.C.P. v. Alabama*, 1958).

This landmark ruling supports the idea that a person's name is a "protected" piece of information owned by the individual, and that the individual has the right to release or not release the information. The legal reasoning behind this case is that there is a vital relationship between freedom to associate and one's privacy in associations. In many cases, individual privacy in group associations may be indispensable to preserving the freedom to *form* associations, this being supported by the Fourteenth Amendment (*N.A.A.C.P. v. Alabama*, 1958).

The case of *Griswold v. Connecticut* (1965) extended the concept of privacy to healthcare information. A Connecticut statute (1958) made it a crime for any person to use any drug or article to prevent conception. The Executive Director of the Planned

Parenthood League of Connecticut and its medical director, a licensed physician, were convicted as accessories for giving married couples information and medical advice on how to prevent conception by prescribing a contraceptive device. The Executive Director and Medical Director sued the state, claiming the statute violated the Fourteenth Amendment, which required the state to use "Due Process" when lawfully removing a person's life, liberty, or property. The court found in favor of the Executive Director of Planned Parenthood and its Medical Director, ruling that the statute violated the Fourteenth Amendment by taking away the individual's freedom to decide conception. It also ruled that it is a person's right to exchange information with their healthcare provider without having that information scrutinized by others. This case was the first time a majority of the court had embraced the concept of patient privacy rights within healthcare. It held that personal privacy in healthcare is protected from government intrusion (*Griswold v. Connecticut*, 1965).

Another landmark privacy case was *Katz v. United States* (1967). Charles Katz was convicted of transmitting wagering information by telephone. Katz's conversations were recorded by FBI agents who had attached an electronic listening device to the telephone booth from which the calls were made. The court ruled that it was unlawful to tap private phone conversations by electronic means without a warrant. This case set the precedent that information shared between persons should be considered private, and that conversations between private persons are protected information under the Fourth Amendment (*Katz v. United States*, 1967).

Like *Katz v. United States* (1967), the case of *Bowers v. Hardwick* (1986) also dealt with the relationship between a private act and public concerns. The Supreme Court

considered the privacy implications of laws banning private consensual sodomy. The court ruled that homosexual sodomy is a public concern when it relates to social decency. The relationship between personal privacy and public concern can be debated on both sides of the field. The offense (legislation) appears to hold to decency and safety concerns, while the defense (individual) maintains privacy as a right that should be granted to each person.

The Wetterling Act (1999), commonly known as "Megan's Law," provides a modern example of the "Greatest Happiness Principle" discussed by John Stuart Mill (1859). Megan's Law requires those who have committed sex crimes against children to be publicly registered. The registry is available for public review. The initiatives behind this act are that sex offenders pose a high risk of re-offending after release from custody, that protecting the public from sex offenders is a primary governmental interest, the privacy interests of persons convicted of sex offenses are less important than the government's interest in public safety, and that the release of certain information about sex offenders to public agencies and the general public will assist in protecting public safety (Wetterling Act, 1999).

One justification often given for the Wetterling Act is families with children who know that John Doe is a convicted sex offender can avoid Doe and keep him away from potential victims. Because the government cannot watch Doe every minute to make sure he is not molesting a child, it enlists the assistance of the civilian population in doing so, therefore making his whereabouts and activities transparent.

The blending of the relationship between what is "private" and what is "public" continues to lead to some confusion in discussions on privacy. *Roe v. Wade* (1973) is by

far the most prominent case in the area of privacy discussions. Roe brought a class action suit challenging the constitutionality of the criminal abortion laws in Texas. These laws limited "proscribing, procuring, or attempting an abortion except on medical advice for the purpose of saving the mother's life" (Texas Penal Code, 1911).

Roe claimed the Texas statutes were unconstitutionally vague, and that they abridged a woman's right of personal privacy, protected by the First, Fourth, Fifth, Ninth, and Fourteenth Amendments. A licensed physician (Hallford) intervened in Roe's case, claiming the Texas statute violated his and his patient's rights to privacy in the doctor-patient relationship, and in his own to practice medicine—rights he claimed were guaranteed by the First, Fourth, Fifth, Ninth, and Fourteenth Amendments. The case was brought before the U.S. Supreme Court, which ruled the Texas statute unconstitutional in that it violated the Due Process Clause of the Fourteenth Amendment. The following was stated by the Supreme Court:

The Constitution does not explicitly mention any right of privacy; the Court has recognized that a right of personal privacy, or a guarantee of certain areas or zones of privacy, does exist under the Constitution. In varying contexts, the Court or individual Justices have, indeed, found at least the roots of that right in the First, Fourth, Fifth, Ninth, and in the concept of liberty guaranteed by the first section Fourteenth Amendments; in the penumbras of the Bill of Rights. These decisions make it clear that only personal rights that can be deemed "fundamental" or "implicit in the concept of ordered liberty," are included in this guarantee of personal privacy. They also make it clear that the right has some extension to activities relating to marriage, procreation, contraception, family relationships, and child rearing and education. . . . This right of privacy, whether it is founded in the Fourteenth Amendment's concept of personal liberty and restrictions upon state action, as we feel it is, or, as the District Court determined, in the Ninth Amendment's reservation of rights to the people, is broad enough to encompass a woman's decision whether or not to terminate her pregnancy. . . . This means, on the other hand, that, for the period of pregnancy prior to this "compelling" point, the attending physician, in consultation with his patient, is free to determine, without regulation by the State that, in his medical judgment, the patient's pregnancy should be terminated. If that decision is reached, the judgment may be effectuated by an abortion free of interference by the State. (*Roe v. Wade*, 1973, pp. 108-109)

The principal thrust of *Roe v. Wade*'s attack on the Texas statutes is that it improperly took away a personal right, in this case the right of Roe to terminate her pregnancy. The court felt this right was embodied in the concept of "personal liberty" found in the Fourteenth Amendment's Due Process Clause; or in personal, marital, familial, and sexual privacy said to be protected by the Bill of Rights and other precedent cases such as *Griswold v. Connecticut* (1965). Historically *Roe v. Wade* has attached itself to the concept of a "woman's right to choose." However, it has more to do with the concept of personal autonomy and the role that privacy plays in a society's right to make choices (Alderman & Kennedy, 1995).

Privacy is not the general concern in the *Roe v. Wade* case; in fact, the courts acknowledge that "the right" is not absolute and is subject to "state interest." The court recognizes the right to terminate first trimester pregnancy under the Fourteenth Amendment's Due Process Clause; however, for subsequent trimesters (second and third), the state can regulate the woman's choice to terminate her pregnancy based on the compelling state interest of the health of the mother. Compelling state interest gives the courts the ability to justify a ruling or nullify a statute depending on whether state interests are at stake (Sargent, 2003). The state should act in the best interest of society.

Utilitarianism has been said to be the philosophy that underlies the modern welfare state (Bentham, 1995). The strength of the utilitarian concept as it applies to *Roe v. Wade* is in the balance between self-interest and the interests of society and its consequences; it recognizes the claimants involved as the client (person), organization, profession, and society. Autonomy of self, development and expression of intellect, and personality are protected by the First Amendment and are absolute, not dependent on

state interests. Freedom of choice in regard to marriage, divorce, procreation, contraception, and education are not absolutes and are subject to state powers and compelling state interests.

The Bill of Rights (1791), as well as the Fourteenth Amendment, has been seen to support the right to privacy of life, possessions, and freedom of choice. Such landmark cases as *N.A.A.C.P. v. Alabama* (1958), *Griswold v. Connecticut* (1965), and *Katz v. United States* (1967) have set the expectation that personal possessions including one's name, release of personal healthcare information, and freedom to make personal medical decisions are rights protected against intrusion from the government.

In addition, the *Roe v. Wade* (1973) case set a precedent that the Constitution's intent was not just to protect individual rights to privacy when it comes to dealing with the government and other citizens, but that the Constitution's true intent included protecting an individual's right to make personal decisions without undue government interference.

Alderman and Kennedy (1995) summarize the writings of Justice Blackmun in the *Roe v. Wade* case:

In a Nation that cherishes liberty, the ability of a woman to control the biological operation of her body . . . must fall within the limited sphere of individual autonomy that lies beyond the will or power of any transient majority. . . . This Court stands as the ultimate guarantor of that zone of privacy, regardless of the bitter disputes to which our decisions may give rise. In *Roe* . . . we did no more than discharge our constitutional duty. (p. 63)

The "zone of privacy" Justice Blackmun refers to continues to expand as the 20th century embraces the Internet, on-line services, and information system technology. Privacy has become both a social and political concern (Federal Register 67, 2002). In the

past few years, numerous privacy laws have been passed focusing on finance, social issues, and education. Following is a sampling of those most pertinent to this study:

1. The Fair Credit Reporting Act (1970) gives fair access and reporting of individual credit information (Hendersen, 1999, p. 87).

2. The Privacy Act (1974) gives the right to any individual to request information from the federal government (Rotenburg, 2000, pp. 57-68).

3. The Family Educational Rights and Privacy Act (1974) gives rights to parents to view educational records of their children and keep others from seeing them (Rotenburg, 2000, pp. 69-74).

4. The Electronic Communications Privacy Act (1986) extended the protections of the Wiretap Act (1968) to prohibit governmental or private interception of cellular communication, computer data transmission, or e-mail (Rotenburg, 2000, pp. 104-140).

5. The Occupational Health and Safety Act (1970) allows workers the ability to examine their occupational health records, therefore opening up the medical record to patient view and critique (Hendersen, 1999).

6. The HIPAA privacy regulation (Kennedy-Kassebaum Bill, 1996) mandates that healthcare entities restrict unauthorized use or disclosure of patient-specific information.

Healthcare and Privacy

Since privacy and its relationship to healthcare is too broad a topic to cover effectively in any one setting, this study will concentrate only on research in the area of consent and autonomy to share information and access to information.

Past studies and legislation on privacy can help us better understand consumer (patient) views on privacy. A number of research studies and judicial cases have contributed to the understanding of privacy and autonomy in healthcare. These include *Warden v. Hayden* (1967), Privacy Act (1974), *Ferguson v. City of Charleston* (2001), Patient Self Determination Act (1990), and Gramm-Leach Bliley Act (1999).

There are also a number of related materials that shed light on this issue. Davis (1977) conducted a qualitative research project that specifically investigated Privacy Act legislation as it pertained to medical information. Healthcare Information Privacy, a poll conducted by Louis Harris and Associates for Equifax, Inc. (1993), identified certain public perceptions about privacy information. Conner (1999) looked at access of information and abuse factors. Borgstede-Mason (1999) examined this in a dissertation entitled *Ethics, Privacy, and Confidentiality Issues Related to the Application of Information Technology in Healthcare*. Fox and Rainie (2001) focused on consumers' use of the Internet for online services and their perceptions of privacy. Slutsman (2004) focused on the HIPAA privacy ruling and the organizational compliance to the ruling.

In the case of *Warden v. Hayden* (1967), Justice Douglas stated the opinion that privacy "means the individual should have the freedom to select for himself the time and circumstances when he will share his secrets with others and decide the extent of the sharing" (p. 324). Historically the medical record has been the sole property of the healthcare provider, and its security controlled by the healthcare entity. Permission to disclose patient-specific information is achieved through the use of an authorized consent form. This authorization has been seen as representing a willingness by the individual to allow his private information to be shared with appropriate entities.

The Privacy Act of 1974 was enacted to control abuses of record keeping by governmental agencies. It was designed to protect individuals from disclosure of confidential information by the Federal government without written consent from the individual giving the information (1974).

Calvin Davis conducted a qualitative research project in 1977, specifically investigating the Privacy Act as it pertained to medical information. The research focused on the nature and extent of individual privacy, conditions in which individual access to personal files is granted, the rights an individual has to revise, add, or delete information from the files, and what rights individuals have concerning the dissemination of information in their personal files (Davis, 1977). This last area of focus (dissemination of information) has particular interest to the current study since it pertains to the concept that healthcare transparency is practiced between consumers and healthcare providers.

Davis's study focused on interviewees from the AMA (American Medical Association), AHA (American Hospital Association), Mayo Clinic, the American Cancer Society, and the Northeast Georgia Community Mental Health Center. Each group was qualitatively surveyed through interviews, then the interviews were transcribed, and results were reported.

Regarding the AMA interviews, Davis (1977) stated the belief of the AMA:

Protection of personal information from the private health care sector would interfere with and jeopardize the quality of medical services. Dr. Boyle pointed out that there are specific types of situations where confidential healthcare information should be allowed to be transferred or released without direct patient consent and authorization. (pp. 87-88)

These situations included releasing information (a) to physicians, dentists, or other medical personnel for diagnosis or treatment; (b) to medical peer review committees; (c)

to a state insurance department or other state agency for purposes of reviewing an insurance claim; (d) to qualified personnel for the purpose of conducting scientific research, management audits, financial audits, program evaluation; (e) by a healthcare provider, as necessary for the provision of healthcare; (f) by an employer for group insurance or workmen's compensation plan; (g) upon the filing of a claim for insurance benefits, between third-party insurers; and (h) between insurers and re-insurers in connection with the underwriting and administration of coverage (Davis, 1977, p. 89).

After interviewing a representative of the AHA, Davis (1977) stated the belief of the AHA:

Strict adherence to the rights of privacy unreasonably limit the hospital's use of its own property—the medical record. . . . The value of the record is greatly reduced and the benefits curtailed if medical record information is allowed to be withheld from hospital use, and its organized medical staff for purposes of continuing patient care, planning health services, conducting bona fide research, carrying out quality assurance and continuing education programs. (p. 97)

Like the AMA, the AHA believed that certain uses of medical information should not require written consent from the patient. Davis listed some of these circumstances, as outlined by Dr. John Porterfield:

1. Requests of physicians and other professional staff for purposes of providing medical care should not require the patient's written consent. The inability to access the record could result in undesirable effects, such as disruption of patient care, prolonged patient stay, and duplication of unnecessary and costly tests.
2. Medical peer review for purposes of reviewing a clinician's work should not require the patient's written consent.
3. Surveys conducted by accreditation bodies, such as Joint Commission on Accreditation of Hospitals, should not require the patient's written consent.

4. Use of patient information for medical research should not require the patient's written consent.

5. Use of patient information for professional education by members of the medical staff should not require the patient's written consent.

6. Use of patient information by administrative staff for purposes of compilation of statistical data for management and planning purposes should not require the patient's written consent (Davis, 1977, pp. 98-103).

Regarding the Mayo Clinic, Davis (1977) utilized statistical data from physicians' records. The study reported that "no single incident in which vital information available to the researchers was used in any manner that was detrimental to the best interests of the patients themselves" (p. 138). It was noted that research conducted by the Mayo Clinic would have been "impossible if proposed regulations extending the Privacy Act of 1974 to the private sector regarding access notification and disclosure had been in force" (Davis, 1977, p. 138).

Regarding the American Cancer Society, Davis (1977) stated that the American Cancer Society maintains a cancer registry for the purpose of research. Intensive investigation necessitated obtaining medical and other information from participants over a period of many years. Davis noted the following:

In all instances great care is taken to maintain the confidential nature of the information. However in order to collect the data, it is necessary to obtain information from many different sources such as: the individual themselves, the physician, hospitals, cancer registries, local and state health departments. In many instances it is virtually impossible to obtain written consent. (pp. 148-149)

Later on, Davis wrote this:

The possibility of obtaining voluntary compliance with the Privacy Act guidelines from currently "unregulated" institutions and researchers will probably depend on the

rationality of such rules. The National Cancer Institute has expressed irritation at having their offices inspected by officials looking for security leaks, and that locks are required on offices and file cabinets containing records which could be of no use to anyone but the researcher. (Davis, 1977, p. 164)

Regarding the Northeast Georgia Community Mental Health Center, Davis's study (1977) focused on the work of Dr. Catherine Rosen, Director of Research. Dr. Rosen was asked by an ACLU attorney whether mental health patients felt they must comply with requests to sign consent forms in order to receive mental health services. It was felt that client compliance in signing had two possible explanations. The first was that "the client complies because he sees the clinic personnel as having legitimate authority, even when the demands of authority conflict with the client's own wishes" (Davis, 1977, p. 172). The second was the fear that "the help they request might be denied if they refuse to sign the consent form" (Davis, 1977, p. 172).

Dr. Rosen conducted a study to see if clients would continue to sign the consent form even if they were told they did not have to submit personal information to the state. New clients were given the consent form, and the following oral statement was made to them:

The state wants to keep a record of name, social security number, and type of problem, of every person. . . . If you sign this paper, you give permission to send your name, social security number, and diagnosis. . . . If you do not sign this paper, this identifying information will not be sent. . . . You will get the same services from us as if you did sign. (Davis, 1977, pp. 174-175)

Group A was presented the entire statement. Groups B and C were given only the first part of the statement and no alternative was given if they did not want to sign. All the clients in B and C signed the consent form. In Group A, 41% complied with signing the consent form. No statistically significant differences were found between those who complied with the signing of the consent and those who did not as it related to age, race,

and income. However the two groups did differ in education and sex. The non-compliers were often female and had completed more years of school (Davis, 1977).

The Rosen Study, as referenced within the Davis study, seems to indicate that consumers (patients) may have the desire to disclose personal information under certain circumstances. The current study seeks to add to the knowledge base determined in the Davis study by exploring more specifically what information patients are willing to share and with whom they are willing to share it, and to examine the correlation (if any) between a consumer's age group and the physician's level of authority when it comes to granting access to healthcare information.

Ferguson v. City of Charleston (2001) is a relatively recent case challenging the rights of consent within a healthcare entity. In March 2001, the courts affirmed the patient's Fourth Amendment privacy rights against information sharing, and upheld the decision to award damage claims to public hospital patients in connection with cocaine-use tests performed on pregnant women. The case involved African American women who were tested through urine samples for cocaine use. Upon discovery of cocaine in the urine, they were arrested. The women filed claims against city officials, hospital personnel, and hospital trustees, stating that "urine drug tests performed pursuant to the search policy constituted warrantless searches in violation of the Fourth Amendment" (*Ferguson v. City of Charleston*, 2001, at 99).

The tests were run at the Medical Center of the Medical University of South Carolina. Since this was a state-run facility, it was identified as a government actor and therefore subject to the Fourth Amendment. The court noted that "the invasion of privacy in this case is far more substantial, a more serious intrusion on privacy than the

unauthorized dissemination of such results to third parties” (*Ferguson v. City of Charleston*, 2001, at 5). The court ruled that in spite of signed consent forms, the plaintiffs’ Fourth Amendment rights were violated because the Medical Center was not acting solely for the best interest of the patients and was collaborating with the police so that patients with positive cocaine test results could be arrested for drug use (*Ferguson v. City of Charleston*, 2001, at 8).

Ferguson v. City of Charleston (2001) implies reevaluation of how informed consent forms are utilized within healthcare entities and what power they carry. Although this case applies only to “government actors” such as state-run healthcare facilities, federal, state, and local governments are becoming more and more involved in the procurement and delivery of healthcare. Thus the application of rules between federal and private entities becomes less clear.

In short, in upholding Fourth Amendment protection of “persons, houses, papers, and effects” against unlawful search and seizure, there may no longer be a clear distinction between public and privately operated healthcare entities, and informed consent may no longer cover the rights of the facility to release patient information to third-party entities. It is unclear at this time whether those healthcare entities that receive governmental funding have sufficient reason to believe they will be held to the Fourth Amendment provisions. However, the case cited may imply that the U.S. Constitution provides patients more protection than the HIPAA privacy regulation. The *Ferguson* case is seen as the first constitutional case awarding civil liability for privacy intrusion arising in a medical information context (*Ferguson v. City of Charleston*, 2001).

The continuing trend in consumer awareness of patient rights within the healthcare setting has prompted additional governmental intervention in assuring the protection of patient information. The Patient Self Determination Act of 1990 outlines how the healthcare consumer (patient) has the right to make certain decisions concerning medical care. These include the right to accept or refuse medical or surgical treatment, and the right to formulate advance directives. Advanced directives outline for the healthcare provider what type of treatment an individual would like to receive if they become unable to make healthcare decisions. For instance, if a person is found unresponsive, an advance directive could stipulate whether they want to have heroic efforts performed on their behalf by the healthcare provider.

Individual hospitals are now recognizing such rights by formally adopting new privacy policies. For example, the University of Pennsylvania has defined as one of its patient rights the right to privacy while in the hospital, and confidentiality of all information and records regarding the patient's care (University of Pennsylvania Bioethics, 1991).

Like the Patient Self Determination Act of 1990, the HIPAA privacy component is a legislative attempt to satisfy those who believe that personal information will be threatened by technological advances within healthcare. The Gramm-Leach-Bliley Act of 1999 combined healthcare systems with banking. Title V of the Act outlined requirements for banks, Healthcare Maintenance Organizations (HMOs), and insurers to disclose how they are using consumers' personal data. It required depository institutions and their subsidiaries to ensure "security and confidentiality of customer records . . .

against any anticipated threats . . . and protect against unauthorized access to, or use of such records” (Gramm-Leach-Bliley Act, 1999, section 6801-6809).

There is no question that as information technology increases, physical access to health information becomes easier. A 1992 opinion survey identified that 79% of Americans agreed that computers have improved the quality of life in our society. However, 68% agreed that the present use of computers constitutes a threat to personal privacy (J. Smith, 1994). This concern about personal privacy related to computer use was a significant increase from the 38% response in the 1974 and 1978 surveys (J. Smith, 1994).

Donna Shalala, former Secretary of Health and Human Services, commented that “our private health information is being shared, collected, analyzed, and stored with fewer federal standards than video store records” (Hendersen, 1999, p. 28).

Yet in spite of Shalala’s comments, public concerns about computer threats to personal privacy do not seem to be as significant when it comes to healthcare entities. *Healthcare Information Privacy*, a 1993 poll conducted by Louis Harris and Associates for Equifax, Inc., identified only 25% of respondents reporting the belief that their medical records had been improperly exposed (Hendersen, 1999, p. 28). The same study showed that only 34% of health professionals believe records were given to unauthorized persons “somewhat often” (Hendersen, 1999). And while the study reported that 85% of the respondents stated that confidentiality of medical information is an important matter, an even greater number (87%) believed that their healthcare providers were keeping medical information confidential (Louis Harris and Associates, 1993).

The Louis Harris poll supports the concept that healthcare entities have developed a reputation for being trusted. The poll seems to indicate that the public supports relevant and appropriate uses of health information, even to the extent of including third-party access, such as insurance companies collecting health and medical information for purposes of issuing policies and determining premiums (Louis Harris and Associates, 1993).

Access to healthcare information by healthcare entities continues to be crucial in maintaining high-quality effective care. Doctors and pharmacists need access to medical records in order to prevent adverse drug reactions. Health Maintenance Organizations need health information in order to control costs and unnecessary treatment. Managers of Medicare programs need access to medical records to assess quality of care and avoid fraudulent Medicare claims. For example, in 1995, "Operation Restore Trust," a 2-year anti-fraud demonstration project undertaken in Florida, Texas, New York, California, and Illinois, identified over \$188 million owed to the federal government for fraudulent healthcare claims (Health and Human Services, 2003).

The National Research Council (1997) acknowledges that a balance between healthcare information access and the protection of patient information is necessary for healthcare entities to operate effectively. The committee found that consumers (patients) had more concern over misuse of information between insurers and vendors than misuse of information between those who were authorized users within the organization.

Unauthorized access by persons other than healthcare professionals is also a concern of healthcare executives (Conner, 1999). In a 1997 survey, the Health Information Management System Society (HIMSS) identified that 41% of the

information executives polled cited internal security breaches as their biggest concern. Executives agree that most intrusions involved inappropriate access by authorized users. Most often these incidents were care providers looking at the charts of someone they knew, such as family members, friends, or co-workers.

Commenting on the 1997 HIMSS survey, Conner (1999) pointed out that only 37% of healthcare organizations had taken steps to protect confidentiality and security of computerized records. Forty-two percent said they were beginning to implement steps, while 21% said they believed implementation of security measures were unnecessary or premature. Of the 79% who said they had implemented or were beginning to implement a security system, only 10% had systems that provided a reliable audit trail to identify who accessed records and what they accessed (Conner, 1999).

A June 1998 survey of 1,063 information security professionals found that over half (54%) had experienced at least one episode of employee access abuse during the past year. This was a 35% increase over the 1997 figures (Conner, 1999). These findings indicate that although executives have identified breaches within healthcare settings, little has yet been done to improve the privacy and safety of patient medical information.

Borgstede-Mason's (1999) qualitative study, *Ethics, Privacy, and Confidentiality Issues Related to the Application of Information Technology in Healthcare*, identified five findings related to healthcare information privacy:

1. There is a major concern for the privacy of the individual patient and the confidential nature of the patient's medical record.
2. The issues that have changed between electronic medical information and paper medical record are how the information is handled, who controls the information,

who needs the information, and how much information is needed by those accessing the Electronic Medical Record.

3. Electronic Medical Records are considered to be very secure. In fact, the information contained in the Electronic Medical Record appears to be much more secure than information in the paper record.

4. Access can be controlled with use of passwords.

5. Backups of the information are kept, so little if any permanent damage could be done to electronic records (p. 17).

Borgstede-Mason's (1999) study was done in three phases. Phase I targeted healthcare industry leaders ranging from physicians and registered nurses to lawyers, government workers, and educators. The 30 participants were interviewed as to what emerging issues were related to information system technologies in health care. Phase II consisted of a focus group that narrowed the issues and identified questions that would be asked of the participating healthcare organizations. Phase III asked the participants at two healthcare institutions the questions that had been identified in Phase II.

Borgstede-Mason (1999) used replication logic that considers multiple cases to see if replications of findings are found. Both institutions were given an oral interview (which contained the main question), a probe question that went deeper into the discussion, and a follow-up question that looked for central themes or asked for elaboration on the answers. Each interview was audiotaped, then transcribed word for word. Data were then grouped and organized according to areas identified. Codes and labels were given to the words so that the data could be retrieved and organized. The codes were then put into Hyperqual-2 for analysis (Borgstede-Mason, 1999). The study

concluded that the core issue of privacy and confidentiality has not changed with increased use of technology, and that the Electronic Medical Record and similar information technology should have a positive impact on healthcare (Borgstede-Mason, 1999).

Another study, undertaken by the Pew Internet and American Life Project, surveyed 12,751 American adults. Of those, 6,413 were Internet users during the months of March through August 2000. The results of this survey identified that 60% of Internet users oppose putting medical records online (Fox & Rainie, 2001).

A separate survey was conducted by Pew Internet and American Life Project in August 2000. It surveyed 521 Internet "health seekers"—people looking for online health advice. Twenty-four percent of respondents said they had read a site's privacy policy to learn how their health information would be used. Fewer than 17% of the health seekers revealed names or personal information, although 21% provided their e-mail address. Of those surveyed who felt revealing health information online could impact decisions about their insurance coverage and employment opportunities if given to insurance providers and employers, a high number identified themselves as African American. Three out of four health seekers (75%) believed healthcare information providers should be allowed to track the activities of those people who visit their sites (Fox & Rainie, 2001).

A phone survey by the Gallup organization of 1,000 participants from the Medic Alert Foundation found that 90% of those respondents trusted their physician to keep information private and secure; 66% trusted hospitals; 42% trusted insurance companies, and 35% trusted managed care companies. Seven percent of respondents were willing to store and transmit personal healthcare information via the Internet (Fox & Rainie, 2001).

Slutsman (2004) conducted a univariate, bivariate, and multivariate study examining the level of organizational and physician efforts to protect the confidentiality of medical information. Her study focused on the HIPAA privacy regulation (2001) and organizational compliance to the ruling. The regulation sought to establish that patient rights are maintained when information is transferred, both within and outside the healthcare setting. The goals of Slutsman's research were to (a) contribute to the understanding of current physician and healthcare organization practices in implementing the practices required by the privacy rule, (b) examine whether the implementation of these practices result in improved confidentiality protection, (c) describe physicians' attitudes towards the Privacy Rule, and (d) explore physicians' experiences regarding confidentiality in patient care (Slutsman, 2004, p. 3).

Slutsman administered a survey to a random sample of physicians from the 2002 American Medical Association master file. Just fewer than 10% (9.1%) of physicians reported their organizations had implemented six of the Privacy Rule practices prior to the deadline of April 14, 2003. Only 20% of physicians stated the Privacy Rule would assist them in protecting their patients' privacy (Slutsman, 2004).

The public outcry for the protection of privacy within our culture in the last decade has led to both judicial and governmental responses. These responses have evoked the idea that privacy is one single issue, and that privacy can be dealt with in a one-size-fits-all approach (Lind, 2002). However, according to the researchers identified within this study, consumers appear to have a broader tolerance for information sharing in the healthcare setting than in personal, financial, or social privacy areas. The challenge for the future appears to be understanding and relating to privacy issues within each of

their domains and separating the concerns over security of information vs. privacy of information. Responses to the research questions in the current study may prove useful in this process by helping determine consumer (patient) attitudes toward privacy of information in healthcare settings.

Transparency

Patient privacy has long been valued by healthcare professionals. The Hippocratic Oath (Hippocrates, 400 B.C.) requires physicians to keep private the affairs of their patients. The *Nurses Code of Ethics* (1953) states that nurses hold in confidence all personal information entrusted to them by their patients (International Council of Nurses, 1953). The Geneva Convention Code of Medical Ethics (Campbell, 1956) identifies the obligation of the healthcare professional to respect the secrets of a patient.

Medical records have long been considered private, since the release of information within such records can alter a person's freedoms, liberties, and possessions. In addition, the privacy rights of the individual have been built within the U.S. judicial system, and such rights are deeply grounded in constitutional intent.

According to the results of a survey by the Pew Trust and Harris Poll, consumers want to believe in the value of "privacy" (Nessen, 2001). But public concerns about privacy are often lumped together into one didactic discussion that covers a broad range of topics. This creates significant problems because, although consumers remain concerned about privacy issues in general (Paul, 2001), their concerns do not appear to be equal for all areas. A poll conducted by the National Consumers League in 2000 showed that consumers are much more concerned about financial, Internet, and identity privacy than about privacy issues related to education, crime, taxes, or healthcare (Paul, 2001).

Lind (2002) states that it is important to separate privacy fears into categories, and not allow one area of privacy abuse to overlap into others. Thus in order to fully understand what is important to the healthcare consumer regarding information privacy, it is imperative to differentiate between public concerns over financial or Internet privacy versus potential privacy issues surrounding healthcare information.

In addition, P. Peters (personal communication, October, 14, 2002) suggests there is some confusion over the desire to protect individual privacy rights compared to public support for transparency as it pertains to social good and personal benefit.

To determine the balance between individual rights and social transparency, examining key judicial cases, feedback regulations, and independent research can help us better understand the dynamic that has developed between these two areas.

Key Judicial Cases Related to Transparency

In *Whalen v. Roe* (1977), there was a perceived conflict between implied patient privacy rights and law enforcement. A New York statute required doctors to transmit a copy of prescriptions for certain dangerous drugs to a state registry. It also required pharmacists to provide the state with a list of recipients who received these dangerous drugs. The forms used for this process (identified as Schedule II) also contained the patient's name, address, and age.

The state maintained that its demand for the names of individuals prescribed these medications was justified for public health and law enforcement reasons. The defendants argued that the statute violated the right to privacy in choosing medication. The concern was that the information could be leaked, and that it could ruin the reputation of the individual receiving the medication.

The court held that the requirements of the statute did not violate a constitutionally protected “zone of privacy.” The court found there was not sufficient evidence to establish an invasion of any rights or liberties based on the Fourteenth Amendment (*Whalen v. Roe*, 1977). In this case, public safety and the need for social transparency outweighed individual privacy rights.

Bartnicki v. Vopper (2001) involved the disclosure of and interception of phone calls, and how this related to First Amendment rights of freedom of speech. This case set a precedent for how the privacy of the individual can be overruled for the sake of a greater public good.

Gloria Bartnicki, a chief union negotiator, used a cell phone to call the union president, Anthony Kane. This cell phone conversation was intercepted and recorded. A copy of the recording was given to the head of the local taxpayer’s organization, Jack Yokum, who recognized the voices. Yokum gave the tape to a local radio commentator, Fredrick Vopper. Vopper aired the tape on his station, then released it to the media.

Bartnicki and Kane sued Yokum, Vopper, and the media. Yokum, Vopper, and the media denied knowing the tape was obtained by an illegal wiretap. The Supreme Court held that Yokum and Vopper were protected by First Amendment freedom of speech, and ruled that the protection of private information “gives way” when compared with important public matters (*Bartnicki v. Vopper*, 2001).

Justice Stevens expressed the main opinion in this case:

Privacy concerns give way when balanced against the interest in publishing matters of public importance. As Warren and Brandeis stated in their classic law review article: “The right of privacy does not prohibit any publication of matter which is of public or general interest” (4 Harv. L. Rev. 193, 214 [1890]). One of the costs associated with participation in public affairs is an attendant loss of privacy. Exposure of the self to others in varying degrees is a concomitant of life in a civilized community. The risk

of this exposure is an essential incident of life in a society which places a primary value on freedom of speech and of press. "Freedom of discussion, if it would fulfill its historic function in this nation, must embrace all issues about which information is needed or appropriate to enable the members of society to cope with the exigencies of their period." (*Thornhill v. Alabama*, 310 U.S. 88, 102 [1940], as cited in *Time, Inc. v. Hill*, 1967)

This case also touched on how technological advances affect privacy. Chief Justice Rehnquist stated in his dissenting opinion that "we are placed in the uncomfortable position of not knowing who might have access to our personal and business e-mails, our medical and financial records, or our cordless or cellular telephone conversations" (*Bartnicki v. Vopper*, 2001).

It should be noted that Judge Rehnquist's comments reflect concerns over privacy of medical records. The HIPAA privacy regulations were designed to restrict free speech in order to protect the individual patient's Protected Health Information (PHI). Yet the First Amendment ruling in the *Bartnicki v. Vopper* case appears to have chosen freedom of speech for the public good over the protection of personal privacy rights. (At the time of this study, HIPAA privacy regulations have not been challenged against First Amendment rights to see if PHI privacy has a place within the First Amendment.)

According to Jorling and Roach (2002), many discrepancies now exist between HIPAA privacy laws and state laws. These discrepancies are creating a competitive threat to both laws.

Preemption is a legal principle that enables one law to control another when both laws concern the same subject. The provisions set forth in the federal privacy regulations are considered the minimum standard for protecting individual health information. Many states actually have more stringent privacy standards related to this same information. Under the principle of preemption, the most stringent law applies. This means that the

state laws on this issue may need to be applied differently than the current federal regulations require. The result, according to Jorling and Roach (2002), will be a myriad of complex evaluations and legal ambiguities that could negatively impact the nation's healthcare practices and policies.

Feedback Regulations and Transparency

There are a number of federal and state "feedback regulations" which support the concept of transparency for the public good. For example, under the Toxics Release Inventory law of 1986, the Environmental Protection Agency (EPA) publishes specific exposure levels for toxic pollutants and the names of companies responsible for these toxins (EPA, 1988). This creates public pressure for manufacturers to be cleaner and more responsible in their operations.

Truth in Lending disclosure laws, which are designed to reveal any patterns of discrimination by race, sex, income, or census tract, are another good example. In the late 1990s, the data showed that Blacks were being turned down 2.7 times as often as Whites for the same income and credit status (Brin, 1998). This created public pressure for banking reform.

In yet another example, the airline industry is required to submit arrival time and lost luggage records to the FAA, which makes this information public. This creates pressure on airlines to improve. Airlines who score high actually use these data for advertising, therefore gaining loyalty from consumers and building greater economic standing.

Automakers must submit accident reports based on model number. Telephone companies must submit reports of service outages. Corporations must submit

compensation rates for top officers. All of this information becomes part of the public record, creating public pressure to make needed improvements.

Finally, at the personal privacy level, Megan's Law (Wetterling Act, 1999) requires the registration of sex offenders living in a community. The courts have ruled that the public's need for this information outweighs the privacy rights of the individuals involved. Also, many states now make public the names of parents who are delinquent on child support payments.

These examples can be seen as indicators of how transparency has created a medium for accountability, improving the marketplace and creating a safer society. David Brin (1998) summarizes:

Notably, public feedback regulations do not generally need coercive bureaucratic meddling, or even lawsuits, to change the behavior of the regulated entity. Rather, the aim is to end asymmetries or inequities in the flow of information, and then let market forces drive the results. (p. 253)

Independent Research and Transparency

Independent research seems to indicate that significant discrepancies exist between an individual's expression of the desire for privacy, and the actual practices of individuals to procure privacy.

For example, most Internet sites offer privacy statements. The American Demographics survey showed that 70% of those polled were willing to "press a button every time they visit a web site, or otherwise use a device," indicating a clear desire for Internet privacy (Paul, 2001, p. 44).

But "pressing a button" provides only limited privacy at best. Procuring true Internet privacy requires more aggressive actions, including setting one's individual

workstation to reject cookies (those small files that many sites slip onto visitors' computers to identify individual users as they browse). According to polls, 60% of users are not even aware of what cookies are, or how they identify personal preferences on the Internet (Nessen, 2001). Only 54% of those who know about cookies take active measures to delete them from their computers (Paul, 2001). And only 10% of users take the steps needed to protect their personal privacy by setting their computers to permanently reject cookies (Fox, 2000). This is just one example of the significant discrepancies that exist between the public's stated desire for Internet privacy and the actual practices that users utilize to understand and/or protect their personal privacy.

A March 2001 Market Facts interactive poll identified similar discrepancies between desire and practice. Sixty percent of respondents stated that "privacy statements" made them feel more comfortable. Yet only 4% of respondents reported they actually read privacy policies every time they visited a new site, and 40% indicated that they read privacy policies "rarely" or "never" (Paul, 2001).

Wiant (2003) studied the effects of privacy policies on information security. She compared the number and seriousness of computer abuse incidents prior to and after the introduction of privacy policies. Her results suggest that regardless of public perceptions, there is no relationship between the introduction of privacy policies and the number of computer abuse incidents. Her study only marginally supported the idea that privacy policies may reduce the severity of computer abuse. She noted the following about privacy legislation:

Legislation may find utility in this study as it is the only known research into the actual effectiveness of information security policy, regardless of the fact that literature alludes to the utility of such policy. If regulations are being passed that implement effective security measures then perhaps other measures should be

undertaken to protect information. Also, all the time invested in creating a policy that may not achieve its intended purpose could be interpreted as a gross waste of time in the face of rising public concern about medical record security. (Wiant, 2003, pp. 127-128)

There also appear to be discrepancies about protecting different types of information based on gender, age, and race. The American Demographic survey (see Table 1) found that respondents believed Social Security numbers were the most important information to protect, and responses from males and females were about equal (96% compared to 97%). But males appeared to be much less concerned about keeping an e-mail address private (63% compared to 70%), and identity theft concerns were much higher among women (57% compared to 51%). In addition, racial minorities were much more concerned than Whites about the possibility of information being used against them (69% compared to 55%) (Paul, 2001).

Table 1

Percentage Scores by Gender and Age on Protection of Private Information

Variable	Gender		Age Group					
	Male	Female	18-24	25-34	35-44	45-54	55-64	65+
Home Address	69	78	84	80	74	74	67	60
Home Phone	72	80	79	80	80	80	69	64
Email Address	63	70	61	74	68	74	74	45
SSN	96	97	86	99	98	97	98	97
Health Information	69	69	57	78	69	77	66	58

Note. Adapted from "American demographics" by P. Paul, July 2001, *Mixed Signals*, pp. 44-49.

There are also discrepancies in how consumers view personal privacy based on age, especially when incentives are involved. Forty-five percent of consumers age 18 to 24 appeared willing to give up some personal privacy information for cash. By contrast, fewer than 10% of those over 55 were willing to exchange information for cash incentives. The offer of free services yielded similar results. Forty-three percent of consumers age 18 to 24 were willing to trade personal information for a free service offering. By contrast, only 13% of those 55 to 64 would make such an exchange (Paul, 2001).

Paul quotes Jan Davis, president of Rocketbridge, a company that provides on-line authentication and verification products for businesses that conduct transactions or transfers of sensitive data:

Privacy is an ideal, but the reality is that we live in a connected society, and if you want to enjoy the benefits of that society, be it access to credit or access to information, you have to be willing to share information. If people perceive that they're getting special benefits they're much more willing to sacrifice privacy. (Paul, 2001, pp. 3-4)

Trust also appears to be a major factor in determining whether individuals will release information. If trust is high, individuals are more willing to share personal information with commercial entities (Milne & Boza, 1999). Horne and Horne (1997) found that "the greater the trust, the less the concern over privacy" (p. 351).

Studies of the banking industry seem to support this concept. Like healthcare entities, the banking industry collects personal information about consumers such as name, address, Social Security number, names of relatives, employers, telephone numbers, license numbers, and birth dates. Yet for many consumers, trust in the banking industry combined with a desire for convenience seems to outweigh concerns about the

privacy of their information. A study by Barry Leeds & Associates showed that 79% of online banking participants would recommend Internet banking to a friend. This was in spite of the fact that less than half the respondents (49%) felt Internet banking was able to keep their information "safe and secure" (Community Banker, 2001).

In a related finding, Norberg (2003) stated that "perception of risk" is directly related to disclosure. The greater the risk perceived, the less the disclosure. Norberg's study looked at the elicitation type and level of trust on actual disclosure, using a 2 x 2 experimental design. He found that "risk mediates the effects of elicitation and trust disclosure, with higher risk leading to less disclosure" (Norberg, 2003, p. 1). However, it is important to note that Norberg did *not* find a direct correlation when it came to the exchange of healthcare information. It appears that when it comes to healthcare, the trust factor may somewhat outweigh the consumer's concerns about risk.

There also appears to be discrepancies when privacy concerns are evaluated on a monetary basis. According to the American Demographics study (Paul, 2001), the willingness to pay a fee for privacy varies significantly from group to group. Minorities appear to be much more willing to pay for protection of personal privacy than Whites (37% compared to 22%). Regions of the country also play a factor. Westerners (30%) and Northeasterners (27%) appear more likely to pay for privacy protection than Southerners (23%) or Midwesterners (18%) (Paul, 2001).

Privacy Versus Transparency

The examples in the previous section highlight the kind of discrepancies that exist between the public's stated desires for privacy and the way they actually behave, as well as significant discrepancies between various groups. In addition, when these behaviors

reflect the concept of social transparency, they tend to further blur the line between what is private and what is public.

Society seems to regularly embrace transparency when it helps achieve certain goals. Some common examples include insuring the public safety (New York City's street surveillance cameras), assisting personal convenience (eBay online shopper network), or offering monetary rewards (reality TV), and increasing social contact as many students do through Face Book.

In her research on the ontology of privacy, Roberts (1993) argued that the dichotomy of public and private ideology causes a separation of one person from the other. She refers to the public and private "bleeding into one another over time" (p. 248), and stated that "given the lack of distinct boundaries or clear conceptions of public and private, neither readily lends itself to understanding" (p. 249). Roberts spoke of privacy as a way of nurturing and sustaining our individuality and roles, as well as maintaining our professional structures so that our economic structures are maintained. She used the example of a grocery clerk maintaining his professional role, as opposed to sharing his family sorrows with patrons and thus disrupting the grocery checkout system (Roberts, 1993).

By contrast, Roberto Unger (1983), a critic of liberal ideology and advocate of communitarian social structures, looked at how these two worlds—the world of privacy and the world of community—could be brought together. He believed this would foster a more complete individual, not confined to a set of roles but free to express his uniqueness and therefore contribute more to humanity. Unger suggested that it might be possible for transparent individuals to have greater intimacies within relationships, and therefore

become more tolerant, complete human beings. He proposed that "individuals would live together in a situation sufficiently varied, intimate and stable to allow them to know and treat each other as concrete persons rather than role occupants" (Unger, 1983, p. 221).

In reference to Roberts's example of the grocery clerk, Unger's theory would suggest that perhaps individuals dealing with the clerk should stop and hear his family sorrows, thus feeling a compassion related to the sorrow of their own lives, and revealing the "sameness" or normality of humanity.

Unger (1983) believed that social transparency could lead to an enriched and shared humanity:

Unless individuals deal with one another in a multiplicity of different ways, they cannot discover the organic unity of each other's personalities. When another is always seen as the performer of a particular role, he must tend to become that role, first in his fellow's eyes, then in his own. . . . The more rigid such outlooks become, the more they hinder the growth of the individual. (pp. 262-63)

In other words, whenever we are able to merge the public and private, the role and the real person, our preconceived biases are challenged and we tend to become more tolerant and compassionate.

Proponents of privacy believe that it is threatened by transparency. Yet the basis for that belief stems from the notion of "selective transparency," transparency that is only imposed on a few. Full transparency means *all* of society is under the same scrutiny and surveillance, and that no one is exempt. Brin (1998) suggests that when transparency is reciprocal and people retain a sense of self-control, distrust and fatalism do not exist. Transparency brings about accountability, and it changes the consciousness of human behavior. Therefore individual rights can be respected and less governmental control is

needed to control the deceit and wrongdoings of the few, thus honoring the privacy of the individual and giving him greater freedom to act as he wills.

Transparency is directly related to accountability. Brettschneider (2002) addresses mutual justification as a means of defending privacy, property, welfare, and life. He uses reciprocity to formulate a theory about fundamental rights that are essential to legitimate societies. He rejects the idea that granting individual rights constrains democracy. The concepts of democracy and individual rights serve each other. The values of mutual justification outline how citizens (in a moral, not legal sense) do not advance their own interests at the expense of others. Rather each citizen is equal, and rights are reciprocal. Therefore, the rights of citizens are basic entitlements (Brettschneider, 2002).

Brettschneider's theory of reciprocal thought and mutual justification relies on accountability for one's actions. Scientists use this theory in "proving" the validity of their research. A scientific theory gains credibility only after it has been tested and retested, surviving repeated attempts to destroy it. Only after attempted annihilation and utter destruction of hypothesis do we come up with accepted models to expand our knowledge base. Brin (1998) makes the following statement about accountability:

Neo-Western civilization has one great trick in its repertoire, a technique more responsible than any other for its success. That trick is accountability . . . making accountability apply to the mighty. . . . Disclosure is the watchword of the age, and politicians have grudgingly responded by passing the Freedom of Information Act (FOIA), truth-in-lending laws, open meeting rules, and codes to enforce candor in real estate, in the nutritional content of foodstuffs, in the expense accounts of lobbyists. (Brin, 1998, p. 11)

Full exposure allows multiple eyes to review, analyze, and credit or discredit. Thus a law, a model, or one's behavior gains credibility through accountability—not as something simply mandated, but as something understood and worthy.

Eugene Senat (2000) supports the concept of accountability:

Public records promote governmental accountability . . . and provide the status of individuals and property, which can help citizens evaluate risk and make intelligent choices regarding a host of life affecting decisions involving business associates, employment relationships, healthcare providers, the education and care of children, marriage and other intimate relationships. (p. 1)

Senat cautions, however, that increasing concerns over privacy are helping lock down government records, therefore denying public access. He quotes Harold L. Cross (1953), general counsel to the American Society of Newspaper Editors: "Public business is the public's business. The people have the right to know. Freedom of information is their just heritage. Without that the citizens of a democracy have but changed their kings" (p. 4).

Meeler (2000) explored the philosophical side of privacy, pointing out that privacy is more than "the right to be let alone." Meeler defined privacy as "the state of existence one chooses to be in." As an example, he refers to a description of Jean Brigg's time with native Utku in the Canadian northlands, and the fact that her fears of loss of privacy were groundless. Meeler quotes Brigg, recounting her experience:

That spot, just the length and breadth of my sleeping bag, very quickly became my spot, and from it I always looked out on the same view. The sameness of it gave me a sense of stability. . . . It even gave me a sense of privacy, since no one ever encroached on my space without permission, and sitting there I could withdraw quietly from conversation into an inner world . . . without disturbance. (Meeler, 2000, p. 2)

Meeler (2000) suggests that what we call "privacy" is really more about autonomy. It is something created and protected within the human soul, as opposed to something granted by someone else, only able to be claimed when offered. He suggests that Supreme Court cases such as *Griswold v. Connecticut*, *Roe v. Wade*, and *Katz v. United States* are really about autonomous choice. In other words, *Griswold's* search and seizure was not about privacy, but about autonomy from government regulation.

Similarly *Roe v. Wade* was about autonomy to make private decisions, and *Katz v. United States* was about autonomy to discuss one's own private affairs without surveillance.

Jarvis-Thomson (1975) stated that the ability to control one's personal privacy independent of governmental intervention is a positive right protected within the Fourth Amendment. Johnson (1975) emphasized how privacy is not an end unto itself, but rather "a set of behavioral strategies designed to attain secondary control over outcomes. . . . Privacy as secondary controls refers to facilitating the attainment of other outcomes or ends" (p. 91). According to Johnson, every individual seeks to attain a given outcome—outcome for the best healthcare, outcome for safer communities, outcome for economic gain, outcome of convenience, and so on. If behavior is altered in order to gain this given outcome, then it is reasonable to assume that each person has a different level of desire for privacy (Johnson, 1975).

Harrison (1993) conducted a quantitative study determining the differences between those who have a strong desire for privacy and those who have little desire for privacy. Primary factors considered were crowding, loneliness, shyness, introversion, and extroversion. Participants were asked to score themselves against a frequency distribution scale. Results of the study determined that socially withdrawn participants have a greater desire for privacy with a strong correlation to shyness and loneliness. Harrison's study found that people vary widely in their motivation for privacy, and that perhaps the greatest contribution is the question of "re-examining the definition of private person and potentially identifying different types of private persons" (p. 45).

Key judicial cases, feedback regulations, and independent research seem to support the concept that the public's expressed desire for privacy often conflicts with

society's need for social transparency. Quoting M. N. Plano, Brin (1998) sums up privacy in our current society:

We are entering the age of mirages, illusions, and make believe. While some people are blinded by all pervading noise, others acquire X-ray eyes, letting them see beyond all the old, traditional walls. For a while, this will create a golden time of opportunity for swindlers, blackmailers, and all kinds of cheaters. But then we will adapt. (Brin, 1998, p. 262)

Summary

The evolution of privacy in society has molded the thoughts of what privacy is and how privacy rights are applied in daily life. The need for privacy was formed out of the individual's need for liberty, life, and ownership (Locke, 1690). The value that possessions brought gave social status and social ranking, separating the powers of the government over the people. The Bill of Rights (1791), specifically the Fourth and Fifth Amendments, protected people's possessions against unlawful violation. Scientific advances in the area of communication and psychology moved the concerns over privacy to greater heights, emphasizing privacy and the desire to protect the secrecy of information (Hendersen, 1999).

Legislation was written to procure the right to privacy. Landmark cases such as *N.A.A.C.P. v. Alabama* (1958), *Griswold v. Connecticut* (1965), *Katz v. United States* (1967), and *Roe v. Wade* (1973) all supported the right to privacy of life, possessions, and freedom of decision making. These landmark cases contributed to the identification of healthcare privacy. As the demands for healthcare access of information grow, so do the controls set in place to ensure security and confidentiality of patient records against unauthorized threats and access.

Many studies contribute to the understanding of healthcare information access and release of information. Davis (1977), Harrison (1993), Borgstede-Mason (1999), and Rosen (2000) all focused on the willingness of patients to release medical information and found that patients are willing to disclose personal information under certain circumstances.

Meeler (2000) suggests that what we call "privacy" is really more about autonomy. It is something created and protected within the human soul, as opposed to something granted by someone else, only able to be claimed when offered. Norberg (2003) stated that "perception of risk" is directly related to disclosure. The greater the risk perceived, the less the disclosure.

Related research has identified a degree of tolerance for release of certain personal information for reasons such as convenience, financial gain, public safety, or the procurement of healthcare services. While consumers speak of their desire for privacy, the reality is that society is interconnected and many benefits come through the sharing of information. If people perceive that they are getting access to such benefits, they appear to be much more willing to sacrifice privacy (Paul, 2001).

Roberts (1993) argued that the dichotomy of public and private ideology causes a separation of one person from the other. Roberto Unger (1983), a critic of liberal ideology and advocate of communitarian social structures, looked at how these two worlds—the world of privacy and the world of community—could be brought together. He believed this would foster a more complete individual, not confined to a set of roles but free to express his uniqueness and therefore contribute more to humanity. Unger

suggested that it might be possible for transparent individuals to have greater intimacies within relationships, and therefore become more tolerant, complete human beings.

Brin (1998) suggests that when transparency is reciprocal and people retain a sense of self-control, distrust and fatalism do not exist. Transparency brings about accountability, and it changes the consciousness of human behavior. Therefore individual rights can be respected and less governmental control is needed to control the deceit and wrongdoings of the few, thus honoring the privacy of the individual and giving him greater freedom to act as he wills.

Brettschneider (2002) addresses mutual justification as a means of defending privacy, property, welfare, and life. Brettschneider's theory of reciprocal thought and mutual justification relies on accountability for one's actions. Eugene Senat (2000) asserts that "public records promote governmental accountability . . . and provide the status of individuals and property, which can help citizens evaluate risk and make intelligent choices" (p. 1).

Historically, healthcare entities have sought to balance individual privacy rights against society's need for social transparency. Such transparency helps maintain public health safety, assists in research initiatives to improve human well-being, and helps assure safe, cost-effective healthcare. As demands for access to healthcare information have grown, so have controls to ensure the security of patient records against unauthorized access. The HIPAA privacy rule seeks to control the access and release of protected health information (PHI) among healthcare entities. Identification of consumer (patient) expectations of what information is desired to protect from healthcare providers

can help clarify and define the need for such privacy legislation among the healthcare market.

The literature review is in no way exhaustive of all privacy legislation or privacy thought and theory. However, an attempt was made to outline the origin of privacy, the judicial response to defining and protecting privacy, the view of privacy from a healthcare perspective, and the discrepancies that exist between the concept of privacy and the practice of transparency. This was done with the hope that clarity can be brought to the discussion on privacy and that both privacy legislation and privacy theory are not lumped together in one didactic discussion, but rather each order by which we live can be evaluated on its own merit. Healthcare privacy legislation is not driven by theories around financial privacy, and sexual privacy rights are not combined with discussions on street corner surveillance systems to control crime. The theories presented around transparency are given as a venue for discussion around how we as a social community view privacy within healthcare. In my research, I will show how a social community practices privacy within healthcare and examine the value placed on privacy by that community.

CHAPTER THREE

METHODOLOGY

Historically, healthcare entities have utilized patient information to maintain patient records, conduct patient billing, and manage overall patient care. The sharing of information between provider, payer, and healthcare professional has always been critical to ensuring cost-effective, high-quality healthcare (Tufts Managed Care Institute, 1998).

In 2001, the Health Insurance Portability Accountability Act (HIPAA) outlined a privacy component identifying 18 types of patient data that healthcare entities were required to protect. These 18 identifiers were labeled as "Protected Health Information" (PHI) (Health Insurance Portability Accountability Act, 1996). The HIPAA privacy component also required healthcare entities to provide opportunity for more informed discussions between patients and providers about how PHI will be used and disclosed within the healthcare system (Federal Register 65, 2000).

Little research has been done to assess the perceptions of consumers (patients) on the importance of protecting their PHI from healthcare providers and others involved in their care. The purpose of this study was to survey a selected population of healthcare consumers (patients) to identify their perspectives on certain personal privacy issues related to the HIPAA PHI indicators. This study focused on four key areas: (a) the type of information the consumer wants to keep private; (b) the relationship of age, nationality,

gender, and authority level in the desire for privacy; (c) who should access information; and (d) the economical priority given to protecting each PHI indicator.

To accomplish the research, a survey was developed to collect the perceptions of consumers (patients) on how they would rate access to each PHI for key individuals involved in their care. This survey tool was distributed through the use of the Internet to individuals who participated in the Carnegie Financial Insurance group plan. The Carnegie Financial Insurance group was chosen as a convenience sample. Individuals were asked to score their responses electronically and submit the results to me electronically.

Research Design

The survey design used for this study is quantitative. Descriptive and Inferential statistics are used to analyze the data. The survey design also included one open-ended question that was analyzed for common themes across the surveyed population.

Population and Sample

A convenience sampling method was chosen as the method for survey distribution. Each survey contained a given explanation of the purpose of the study and how the research was to be utilized. Surveys were electronically recorded. The participants were asked to record their responses and submit the survey back to me electronically. The survey was reviewed and approved for distribution by the Institutional Review Board of Andrews University. A copy of the survey is included in the Appendix and can also be found on the Internet at <http://www.tkgnet.com/dlksurvey/survey.asp>.

Research data were collected through the use of the Internet, utilizing the Carnegie Financial Insurance e-mail distribution list. The Carnegie Financial Insurance group offers health insurance to participants nationwide. The Carnegie organization maintains an e-mail list directory which serves as a communication tool for participants in their program. This distribution list includes 628 participants ranging in age from 18 to 82 years.

The population to be surveyed consisted of all individuals participating in the Carnegie Financial Insurance plan. All participants were sent the survey via e-mail. Each participant was given information pertaining to the intent of the study, including benefits I may find through the participant's responses. Benefits include the potential for restructuring public policy as it relates to privacy within healthcare based on establishing a value for each PHI. Each participant was informed that the information contained in the survey would be private, and that no reference leading to identification of any individual participant would be made in the findings of the study.

The survey included detailed instructions on how to submit answers. The survey was designed so that each question could be answered with a simple mouse click within the radio buttons corresponding to that question. The survey was also designed so that multiple responses to the same question are not possible. Consent to participate in the study was confirmed by submission of the completed survey electronically to me.

Question 7 of the survey was a "free text comment field" designed to solicit participant opinions on what other information they believe should be kept private. The participant was free to enter any data within this field. Participants who included comments in Question 7 were assumed to have basic word-processing skills.

Following completion of the survey, the participant was given a "submit" button. Selecting the submit option electronically registered the survey and its results in an Access database. Results were then compiled and entered into SPSS for statistical analysis. Question 7 was qualitatively recorded in thematic categories. Following the receipt of the first round of surveys, a follow-up email was sent as a reminder to complete the survey and submit the results. The first round of receipts yielded 209 surveys, a response rate of 33%, the follow-up email reminding the respondents to send in their surveys yielded an additional 9, with a total response rate of 35%.

Instrumentation

The survey consists of nine quantitative questions and one open-ended question. The participants were asked to record their responses to all 10 questions. The survey is broken down into six quantitative response questions, one open ended opinion question, and three quantitative demographic questions. Each of the six quantitative response questions required an answer based on the following Protected Health Information (PHI) indicators: (a) name; (b) address (including street address, city, county, zip code, and equivalent geocodes); (c) names of relatives; (d) name of employers; (e) birth date; (f) telephone numbers; (g) fax numbers; (h) electronic mail addresses; (i) Social Security number; (j) medical record number or (k) health plan beneficiary numbers; (l) account number; (m) certificate/license number; (n) any vehicle or other device serial number; (o) web Universal Resource Locator (URL)/ Internet Protocol (IP) address; (p) finger or voice prints; (q) photographic images (Privacy Rule, 2002).

Question 1 of the survey asked the participant whether she believes her doctor has the ultimate authority when it comes to her healthcare. Question 2 asked the participant to

score each PHI based on how accessible he believes it should be to his healthcare team. Question 3 asked the participant to score each PHI based on how much she believes she should be able to limit access to that specific PHI. Question 4 asked the participant to score each PHI based on how accessible he believes it should be to his insurance provider. Question 5 asked the participant to score various types of persons: family members, healthcare providers, researcher, law enforcement, pharmacist, and pastor (religious advisor) for how accessible health information should be. Question 6 asked the participant to score the monetary value of protecting the privacy of each PHI. The scale of measurement is low (\$), medium (\$\$) and high (\$\$\$). Question 7 asks the participant to "free text" any additional information he believes should be kept private. Question 8 asked for the participant's age. Question 9 asked for the participant's gender. Question 10 asked for the participant's race.

Participants were asked to score the first five questions using a scale of 1 to 5. This form of measurement is based on the Likert Scale. The Likert Scale is divided into five categories:

1 = Always

2 = Mostly

3 = Sometimes

4 = Almost Never

5 = Never.

Question 6 used the dollar sign to convey values. The dollar sign is universally recognized as a monetary measurement tool (Marriott International, 2001).

Question 8 used the age categories of "18-30," "31-45," "46-60," "61-70," and "71-over."

Question 10 used the following race divisions: "White/Caucasian," "Hispanic," "Asian," "Black/African American," and "Native American." It also offered participants the option of filling in another racial group under "Other," or clicking a button to indicate, "I prefer not to answer this question."

The survey concludes with a "free text" area for additional participant input and an area where participants may enter their name, e-mail, and phone number if they wish to be contacted by me to discuss their views.

Quantitative components of this study (Questions 1-6 and Questions 8-10) were entered into a statistical software program for statistical analysis. Question 7 was recorded in the study findings as word analysis and placed into thematic categories.

Data Gathering

Survey data were distributed electronically, and upon completion each survey was sent electronically via e-mail to me. The survey tool was electronically transcribed with the use of computer coding. A computer technician within the Carnegie Financial Insurance organization developed the survey coding. With the exception of Question 7, which is a "free text" scrolling field, the survey contains a computer code that allows only one answer per question. Upon completion of the electronic survey and the selection of the submit button, the program submits the survey electronically. The results were electronically aggregated within an Excel spreadsheet. The data were then transcribed into SPSS for data analysis.

Pilot Study

I developed a survey tool to analyze the content validity of each question as it related to the specific aspect of the HIPAA privacy regulation (Kennedy-Kassebaum, 42 U.S.C. § 1397ii 1996). The survey tool was tested in a pilot study consisting of 42 participants chosen by me using a convenience sampling method. Individuals who received the surveys completed them independently, without my instruction or observation. Responses were mailed to me.

Twenty-seven of the surveys were returned, which is a 64% return rate. The survey consisted of nine questions total. Five of the survey questions asked the participant to score each of the Protected Health Information (PHI) indicators based on how accessible he believed it should be. The PHI indicators were obtained from the HIPAA regulation document (Federal Register 65, 2000). I constructed questions related to PHI from the comments submitted by the general public within the Federal Registry comment section (Federal Register 67, 2002).

The survey also contained two demographic questions. One of them asked the participant to place himself in one of seven age groups, organized in seven categories (18-25, 26-30, 31-40, 41-50, 51-60, 61-70, 70 and over). The other demographic questions related to nationality, asking the participant to place herself in one of five categories (Caucasian, Hispanic, Asian, Black/African American, Native American).

Another question centered on how much physician authority was granted by the participant to those giving professional patient care. This question was derived from my anecdotal observations within the clinical setting that "older" persons appeared to give higher authority to their professional care providers than their "younger" counterparts.

The last question in the survey was a free text question asking the participants to list other information they thought should be kept private.

The pilot study was of significant benefit to the development of the current survey instrument in that it allowed me to evaluate respondents' perception of individual questions. It became apparent that the instrument needed some clarification in order for participants to understand the intent of the questions. These clarifications included a better visual layout of the questions and scoring, as well as using terms that were more clearly defined.

Research questions were also evaluated for the ability to do descriptive statistics. Additional descriptive variables were added to the current survey instrument in order for comprehensive data analysis to be meaningful to me. Improvements to the current instrument based on the knowledge acquired from the pilot study resulted in what should be a more valid and statistically sound instrument.

Upon review of the participants' completed surveys within the pilot instrument, it was determined that a number of the questions needed to be restructured to include better definition of the terms. The term "family member" was broken down into five more specific categories: Spouse, Parent, Significant Other, Child, and Sibling. The term "Health Provider" was broken down into three categories: Doctor, Nurse, and Therapist. Key words such as "limit," "viewable," and "money" were bold-faced to draw attention to the intent of the question.

I also found that clarification was needed for the PHI elements "Web URL," "Internet IP Address," "Any vehicle or other device serial number," and "Certificate/license number." Many of these items were left unanswered in the pilot

study. Therefore the PHI element "Any vehicle or other device serial number" was changed in the current survey instrument to read "License (any) Number" and "Vehicle Serial Number." For simplification the terms "Web URL" and "Internet IP Address" were combined in the current instrument as "Web Address."

Participants noted that the pilot instrument was visually difficult to read. Tables with their related columns for each question were cumbersome to use since each question also contained the 18 PHI indicators. It was difficult for participants to keep their place as they moved horizontally and vertically around the columns. To help with orientation, PHI indicators were alternately shaded and un-shaded in the revised survey instrument.

Some of the questions contained in the original pilot study were not suitable for comprehensive descriptive statistics. Each PHI question was altered to reflect the commonly used Likert Scale of measurement (1 = always, 5 = never). Responses to the questions were also changed to include all ordinal data for all PHI-related questions.

I received feedback from pilot participants that gender should be added to the survey. This could help expand the interest of the research to gender classes. Gender was added to the demographic section of the revised survey instrument. Race was divided into categories including White/Caucasian, Hispanic, Asian (Pacific Island), Black/African American, Native American, and Other. An additional category was added allowing the participant to decline from listing race by stating "I prefer not to answer this question." Age categories were condensed from the original six categories down to five categories: 18-30, 31-45, 46-60, 61-70, 71 and over.

The new survey tool was also tested for content validity. Each survey question was analyzed to determine if the intent of the questions was properly understood. I felt

the biggest risk to the survey was that terms used within the question were not collectively understood by participants. I wanted to be sure that the terms within the survey matched the understanding of participants taking the survey. Analysis of the survey questions for content validity was done through qualitative measures. All participants of the pilot survey were asked to participate in a review committee to validate the new survey tool. Ten participants responded with interest. This group was labeled the "validity group." Interviews were conducted with 10 of the participants who completed the pilot survey. Each participant was asked to give his/her understanding of the question, and the responses were matched against a given set of criteria and the meanings of the terms listed within the question. Responses were as follows:

Question 1: Do you believe that your doctor is the ultimate authority concerning your healthcare? The phrase "ultimate authority" may have been misunderstood. When qualitatively questioned about the term "ultimate authority," 8 out of 10 participants in the survey validity group used words such as "rights," "knowledge," and "purpose" to describe its meaning.

Question 2: Do you believe that your healthcare team (those caring for you when you are in a care facility) should be able to see the following? The phrase "healthcare team" may not have been understood. When qualitatively questioned about the term "healthcare team" and what meaning it held for them, the 10 participants in the survey validity group responded with descriptions such as doctor, nurse, or dietician. In addition, when participants of the validity group were asked to list any term from the PHI that they did not understand, the most misunderstood terms included "Web URL," "Internet IP

Address,” “Any vehicle or other device serial number,” “Certificate/license number,” “Photographic images,” and “Finger, Voice print.”

Question 4: Should the following information be viewable by your healthcare insurance providers? The word “viewable” may have been misunderstood. When qualitatively questioned about the term “viewable” and what meaning it held for them, common themes that arose included “able to see,” and “information given to.”

The scoring method for each question of the survey tool was also assessed for reliability. The 10 participants of the validity test group were asked to identify how easy the scoring tool was to use. Six out of 10 participants stated that the scoring method was difficult to follow at times because of all the PHI listings. Their comments reflected the fact that they had to repeatedly look back to the top of the grid to see what the scoring value meant.

The same 10 participants were asked to retake the survey to assess reliability. The initial pilot did not identify the participants surveyed, therefore a one-to-one match could not be performed. The test/re-test methodology was used to determine similarities between Group 1 (initial pilot group) and Group 2 (validity group).

Research Questions

As has already been stated before, healthcare entities utilize patient information to maintain patient records, conduct patient billing, and manage overall patient care. The sharing of information between provider, payer, and healthcare professional has always been critical to ensuring cost-effective, high-quality healthcare (Tufts Managed Care Institute, 1998).

However, the privacy component within the HIPAA regulation gives patients the authority to restrict use or disclosure of personal information. The proposed research questions explored the consumer's (patient's) perspective regarding what Protected Health Information (PHI) is important to protect:

1. What components of the Protected Health Information do patients want to keep confidential from their healthcare providers?
2. What is the relationship to demographic factors in desire for privacy?
3. What is the relationship between authority ascribed to physicians and who has access to healthcare information?
4. What is the level of financial commitment given by the patient to protect each element of Protected Health Information mandated by the privacy rule?
5. What other information do the respondents think should be kept private?

Analysis of Data

Research question 1: "What components of the Protected Health Information do patients want to keep confidential from their healthcare providers?"

This research question was answered by analyzing survey Question 2 (Do you believe that your healthcare team, those caring for you when you are in a care facility, should be able to see the following information?). The Likert Scale of measurement was used. Data were analyzed utilizing the mean score. The mean score was organized in the following Likert Scale categories: 1-1.79 = *Always*, 1.80-2.59 = *Mostly*, 2.60-3.39 = *Sometimes*, 3.40-4.19 = *Almost Never*, 4.20-5.00 = *Never*.

Research question 2: What is the relationship between demographic factors and the desire for privacy? This research question was answered by analyzing survey

Question 8 (“What is your present age?”), Question 9 (“What is your gender?”), and Question 2 (“Do you believe that your healthcare team, those caring for you when you are in a care facility, should be able to see the following information?”). My null hypotheses are as follows:

1. There is no difference between age categories in determining what Protected Health Information is desired to protect from a healthcare provider.

2. There is no difference between gender categories in determining what Protected Health Information is desired to protect from a healthcare provider.

One-way Analysis of Variance utilizing Tukey HSD for post-hoc analysis to determine significance difference at .05 level was used to observe the relationship of age and gender for each PHI indicator as it relates to healthcare member access.

Research question 3: What is the relationship between authority ascribed to physicians and who has access to healthcare information? This research question assessed whether there is any difference between granting authority and willingness for full access as determined by age. The research question was answered by analyzing survey Question 1 (“Do you believe that your doctor has the ultimate authority when it comes to your healthcare?”), Question 5 (“How comfortable are you with the following persons having access to your Health Information?”), and Question 8 (“What is your present age?”). My hypotheses are as follows:

1. There is no difference among patients who ascribe various levels of authority to their physicians and their comfort level with other people having access to their health care information.

2. There is no difference between younger and older patients regarding their comfort level with other people having access to their healthcare information.

3. There is no interaction between patients who ascribe various levels of authority to their doctor and the age of the patient regarding their comfort level with other people having access to their healthcare information.

Two-Way Analysis of Variance was used to determine the main effect and interaction effect of age and authority to access of health information by insurance provider, spouse, parent, significant other, child, siblings, doctor, nurse, therapist, researcher, law enforcement, pharmacist, and pastor.

Research question 4: What is the level of financial commitment given by the patient to protect each Protected Health Information mandated by the privacy rule? This research question was answered by analyzing survey Question 6 ("How much of your own money would you invest in protecting the privacy of the following Protected Health Information?"). Data were analyzed utilizing frequency distribution through response categories of low (\$), medium (\$\$), and high (\$\$\$). Each PHI had a frequency distribution of low, medium, or high. The PHI containing the highest score (\$\$\$) was considered the highest value. It should be noted that no actual dollar value has been given to any category within this study.

Research question 5: What other information do the respondents think should be kept private? This research question was answered utilizing qualitative methodology by analyzing Question 7 ("What other information do the respondents think should be kept private?"). The research question was answered by first compiling the text answers that

have been entered in the free text box by the participants, and then organizing them into thematic categories. The categories are listed in the findings of my study.

Limitations of the Study

It is recognized that the current study poses some limitations that threaten the internal validity of the study. These limitations are starting points to opportunities for continued research:

1. It will not be possible to identify if participants really understood the questions. This poses a challenge to internal validity.
2. It will not be possible to identify if participants knew how to properly use a computer to score and record their answers. This also poses a challenge to internal validity.
3. It will not be possible to generalize widely from the sample. This limits the sample's external validity.
4. It will not be possible to verify who answered the survey questions.

Summary

The methodology used to analyze the data included both descriptive and inferential statistics, including One- and Two-Way ANOVA. The survey was distributed electronically to the participants of the Carnegie Financial Insurance group. The survey instrument consisted of nine quantitative questions and one open-ended question. A 5-point Likert scale of measurement was used as well as each participant was asked to provide demographic information such as age and race. Participants' responses were submitted electronically and entered into SPSS for data analysis.

CHAPTER FOUR

RESULTS

The overall purpose of this study was to survey a selected population of healthcare consumers (patients) to identify their perspectives on certain personal privacy issues related to the HIPAA (Health Insurance Portability Accountability Act) privacy rule. The intention of the study was to find what type of information the consumer wants to keep private; the relationship of age, nationality, gender, and authority level in the desire for privacy; who should access information; and the economical priority given to protecting each PHI indicator.

The study explored the consumer's (patient's) perspective regarding what Protected Health Information (PHI) is important to protect:

1. What components of the Protected Health Information do patients want to keep confidential from their healthcare providers?
2. What is the relationship to demographic factors in desire for privacy?
3. What is the relationship between authority ascribed to physicians and who has access to healthcare information?
4. What is the level of financial commitment given by the patient to protect each element of Protected Health Information mandated by the privacy rule?
5. What other information do the respondents think should be kept private?

Using a survey instrument (see Appendix), the participants of the Carnegie Financial Insurance group were asked to give their response to six quantitative response questions, one open-ended opinion question, and three quantitative demographic questions utilizing the Likert Scale of measurement for all quantitative questions and free text for the open-ended question.

The survey was sent electronically to all participants of the Carnegie Financial Insurance Group distribution listing nationwide. The sample surveyed consisted of 628 participants ranging in age from 18 to 82 years, and 209 surveys were returned for a response rate of 33%. A follow-up email was sent to respondents requesting surveys to be completed and returned; an additional 9 surveys were received, with a response rate of 35%. Table 2 shows the total number of respondents for the three demographic variables represented in the survey. It should be noted that not all questions were answered by every respondent, and therefore variability in the demographics exists.

Data results from the 218 surveys were analyzed utilizing the software program SPSS. Both One-Way and Two-Way Analysis of Variance were utilized for the four independent variables: age, nationality, gender, authority level and the 17 selected dependent variables: (a) name; (b) address (including street address, city, county, zip code, and equivalent geocodes); (c) names of relatives; (d) name of employers; (e) birth date; (f) telephone numbers; (g) fax numbers; (h) electronic mail addresses; (i) Social Security number; (j) medical record number or (k) health plan beneficiary numbers; (l) account number; (m) certificate/license number; (n) any vehicle or other device serial number; (o) web Universal Resource Locator (URL)/ Internet Protocol (IP) address; (p) finger or voice prints; (q) photographic images.

Table 2

Survey Demographic Results

Demographic	No. of Respondents
<i>Age</i>	
18 -30	24
31 - 45	74
46 - 60	101
61 - 70	13
71 - over	0
<i>Gender</i>	
Male	111
Female	101
<i>Race</i>	
White/Caucasian	178
Hispanic	6
Asian	5
Black/African American	13
Native American	0
Other	1
Prefer not to answer	10

Research Question 1

Five major research questions were addressed in this study. The first of these questions was, What components of the Protected Health Information do patients want to keep confidential from their healthcare providers?

On the survey instrument, participants were asked to rate each dependent variable based on their belief that their healthcare team (those caring for you when you are in a care facility) should be able to see the following: (a) name; (b) address (including street address, city, county, zip code, and equivalent geocodes); (c) names of relatives; (d) name of employers; (e) birth date; (f) telephone numbers; (g) fax numbers; (h) electronic mail addresses; (i) Social Security number; (j) medical record number or (k) health plan beneficiary numbers; (l) account number; (m) certificate/license number; (n) any vehicle or other device serial number; (o) web Universal Resource Locator (URL)/ Internet Protocol (IP) address; (p) finger or voice prints; (q) photographic images.

The 5-point Likert Scale was utilized, where 1 = *Always*, 2 = *Mostly*, 3 = *Sometimes*, 4 = *Almost Never*, 5 = *Never*. For purposes of this analysis, the following criteria were used to determine the degree to which participants believe their healthcare team should be able to see the 17 selected Protected Health Information indicators. If the overall mean scores ranged from 1–1.79, then the belief is the healthcare team should “always” be able to see the indicated Protected Health Information. If the mean scores were between 1.80 and 2.59, the belief is that information should “mostly” be available to healthcare providers. If the mean scores fell in the range of 2.60–3.39, the belief is that the information should “sometimes” be available. A range of 3.40–4.19 equates to the belief that healthcare providers should “almost never” be able to see the 17 Protected Healthcare Information. Finally, a rating in the 4.20–5.00 range was perceived to be “never” allowing healthcare providers access to Protected Health Information. The higher the mean score, the more desire for privacy with the 17 Protected Health Information indicators.

When using the criteria established above to determine the degree of belief each participant has towards the healthcare team being able to view the 17 selected Protected Health Information indicators, data in Table 3 indicate that for the overall mean score for the selected Protected Health Information indicators, electronic mail addresses, license number, vehicle serial number, web address, finger or voice print were perceived to be either "almost never" or "never" allowed to be viewed by a healthcare team member, therefore indicating a high desire for privacy with these Protected Health Indicators.

The Protected Health Information listed according to greatest concern, include: email (3.43), license number (3.90), finger or voice print (4.00), web address (4.23), vehicle serial number (4.45). The remaining Protected Health Information indicators, which scored "always," "mostly," and "sometimes" in allowing healthcare team members access to Protected Health Information, were name (1.16), address (2.38), names of relatives (2.40), name of employers (3.22), birth date (1.62), telephone numbers (2.38), fax numbers (3.23), Social Security number (3.34), medical record number (1.72), health plan beneficiary numbers (2.17), account number (2.14), and photographic images (3.21), indicating that a low level of privacy is desired. These data points are summarized in Table 3.

The analysis shows that 5 out of the 17 Protected Health Information indicators are desired to be protected and therefore considered private to the respondent. Vehicle serial number and web address were given the highest priority for keeping private from healthcare team members. These data are summarized in Table 3.

Table 3

Components of PHI That Patients Want Healthcare Providers to Have Access To

PHI	Overall Mean Score	Degree of Access/View
Name	1.16	Always
Address	2.38	Mostly
Relatives	2.40	Mostly
Employers	3.22	Sometimes
Birth Date	1.62	Always
Telephone	2.38	Mostly
Fax	3.23	Sometimes
Email Address	3.43	Almost never
SSN	3.34	Sometimes
MRN	1.72	Always
HPN	2.17	Mostly
Acct. No.	2.14	Mostly
License No.	3.90	Almost never
Vehicle Serial No.	4.45	Never
Web Address	4.23	Never
Finger/Voice Print	4.00	Almost never
Photo Images	3.21	Sometimes

Note. SSN= Social Security number; MRN= medical record number; HPN= health plan number.

Research Question 2

The second research question under consideration in this study was, What is the relationship between demographic factors and the desire for privacy?

In developing appropriate hypothesis statements related to Question 2, there exist three independent variables: age, nationality, gender. The dependent variables are each of the 17 selected Protected Health Information indicators each analyzed separately: (a) name; (b) address (including street address, city, county, zip code, and equivalent geocodes); (c) names of relatives; (d) name of employers; (e) birth date; (f) telephone numbers; (g) fax numbers; (h) electronic mail addresses; (i) Social Security number; (j) medical record number or (k) health plan beneficiary numbers; (l) account number; (m) certificate/license number; (n) any vehicle or other device serial number; (o) web Universal Resource Locator (URL)/ Internet Protocol (IP) address; (p) finger or voice prints; (q) photographic images. The higher the mean score, the more desire for privacy.

The results collected on type of nationality revealed that the sample size was not evenly distributed, therefore analysis on the results by nationality was omitted from the study. The perspective on HIPAA PHI and the relationship to nationality will be considered open for future research. Only age and gender were considered for addressing research question 2, the following two hypotheses were tested for age and gender:

Hypothesis 1: There is no difference between age categories in determining what Protected Health Information is desired to protect from a healthcare provider. The hypothesis was tested by analyzing the responses to survey Question 8 ("What is your present age?") and Question 2 ("Do you believe that your healthcare team, those caring

for you when you are in a care facility, should be able to see the following information?”).

A One-Way Analysis of Variance was used to test for significant differences among the age groups and each Protected Health Information indicator. As seen in Table 4, there was a significant difference among the age groups tested, utilizing a significance level of .05. Subjects were divided into four groups according to their age (Group 1: 18-30; Group 2: 31-45; Group 3: 46-60; Group 4: 61-70; there were no respondents over age 70). There was a statistically significant difference at the $p < .05$ level in the belief that the healthcare team should be able to see each PHI for the four age groups. Thirteen of the 17 dependent variables were considered significant, therefore Null Hypothesis 1 was rejected. Significant differences existed among the groups for names of relatives ($p < .001$), name of employers ($p < .008$), birth date ($p < .042$), telephone numbers ($p < .001$), fax numbers ($p < .001$), electronic mail addresses ($p < .015$), Social Security number ($p < .050$), medical record number ($p < .050$), health plan beneficiary numbers ($p < .012$), certificate/license number ($p < .001$), vehicle/device serial number ($p < .006$), web Universal Resource Locator (URL)/ Internet Protocol (IP) address ($p < .043$), and photographic images ($p < .002$). These data are summarized in Table 4.

A multiple comparisons utilizing the Tukey HSD test shows significant differences between the four groups at the $p < .05$ level. Data are displayed in Table 5.

Group 1 indicated significantly less desire for privacy than all three other groups in certificate/license number. Group 1 showed less desire for privacy than group 2 on web address and photographic images as well as significantly less privacy than groups 2 and 3 for names of relatives, telephone numbers, fax numbers, electronic mail addresses,

certificate license number, and vehicle/device serial number. Group 1 indicated significant less desire for privacy than group 4 on certificate/license number, vehicle device/serial number and photographic images.

Groups 2, 3, and 4 did not differ significantly amongst themselves in any of the Protected Health Information indicators. These data are summarized in Table 5.

Table 4

ANOVA for Hypothesis 1—Age

PHI	Age Group								df	F	p
	18-30		31-45		46-60		61-70				
	M	SD	M	SD	M	SD	M	SD			
Name	1.04	0.20	1.28	0.80	1.12	0.43	1.07	0.27	3,207	1.75	.158
Address 1.87	1.07	2.59	1.34	2.41	1.40	2.07	1.18	3,207	2.01	.113	
Relative 1.65	0.77	2.71	1.16	2.42	1.19	2.00	1.15	3,206	5.66	.001***	
Employer	2.56	0.09	3.55	1.19	3.17	1.31	3.07	1.38	3,206	4.05	.008**
Birth Date	1.16	0.38	1.77	0.98	1.65	1.01	1.38	0.86	3,206	2.78	.042*
Telephone	1.57	0.72	2.77	1.34	2.32	1.39	2.30	1.18	3,205	5.59	.001***
Fax	2.08	1.01	3.52	1.30	3.31	1.44	3.07	1.11	3,207	7.30	.001***
Email	2.62	1.24	3.67	1.30	3.46	1.46	3.38	1.12	3,207	3.58	.015**
SSN	2.79	1.10	3.66	1.30	3.24	1.51	3.38	1.70	3,207	2.65	.050*
MRN	1.37	0.64	1.94	1.15	1.69	0.99	1.38	0.76	3,206	2.65	.005*
HPN	1.45	0.72	2.41	1.28	2.15	1.25	2.23	1.42	3,207	3.70	.012**
Acct. No.	1.70	0.95	2.25	1.27	2.14	1.38	2.41	1.56	3,203	1.23	.298
License No.	2.87	0.99	4.00	1.28	4.05	1.18	4.15	0.98	3,206	6.84	.001***
Vehicle No.	3.83	1.09	4.52	0.88	4.53	0.95	4.69	0.48	3,206	4.21	.006**
Web Address	3.66	1.30	4.35	1.01	4.25	1.08	4.46	0.66	3,205	2.76	.043*
Finger/Voice	3.54	1.17	4.17	1.27	3.91	1.24	4.46	0.66	3,206	2.40	.069
Photo Image	2.39	0.98	3.52	1.31	3.13	1.30	3.53	1.19	3,206	5.14	.002**

Note. N=209-211. SSN= Social Security number; MRN= medical record number; HPN= health plan number.

* $p < .05$. ** $p < .01$. *** $p < .001$.

Table 5

Tukey HSD—Privacy Desired for Each PHI by Age Group

Dependent Variable	(I) Age	(J) Age	Mean	Mean Difference (I - J)	Std. Error	Sig.
HCRELAT	1.00	2.00	2.71	-1.06404*	0.27362	0.001***
		3.00	2.42	-0.76783*	0.26505	0.022*
		4.00	2.00	-0.34783	0.39770	0.818
	2.00	1.00	1.65	1.06404*	0.27362	0.001***
		3.00	2.42	0.29622	0.17575	0.334
		4.00	2.00	0.71622	0.34468	0.164
	3.00	1.00	1.65	0.76783*	0.26505	0.022*
		2.00	2.71	-0.29622	0.17575	0.334
		4.00	2.00	0.42000	0.33792	0.600
	4.00	1.00	1.65	0.34783	0.39770	0.818
		2.00	2.71	-0.71622	0.34468	0.164
		3.00	2.42	-0.42000	0.33792	0.600
HCTELE	1.00	2.00	2.77	-1.22860*	0.30578	0.001***
		3.00	2.32	-0.78486*	0.29647	0.043*
		4.00	2.30	-0.76603	0.44828	0.322
	2.00	1.00	1.54	1.22860*	0.30578	0.001***
		3.00	2.32	0.44374	0.20047	0.123
		4.00	2.30	0.46258	0.39147	0.639
	3.00	1.00	1.54	0.78486*	0.29647	0.043*
		2.00	2.77	-0.44374	0.20047	0.123
		4.00	2.30	0.01884	0.38424	1.000
	4.00	1.00	1.54	0.76603	0.44828	0.322
		2.00	2.77	-0.46258	0.39147	0.639
		3.00	2.32	-0.01884	0.38424	1.000
HCFAX	1.00	2.00	3.52	-1.44369*	0.31346	0.001***
		3.00	3.31	-1.22667*	0.30331	0.001***
		4.00	3.07	-0.99359	0.45953	0.137
	2.00	1.00	2.08	1.44369*	0.31346	0.001***
		3.00	3.31	0.21703	0.20462	0.714
		4.00	3.07	0.45010	0.40129	0.677
	3.00	1.00	2.08	1.22667*	0.30331	0.001***
		2.00	3.52	-0.21703	0.20462	0.714
		4.00	3.07	0.23308	0.39342	0.934
	4.00	1.00	2.08	0.99359	0.45953	0.137
		2.00	3.52	-0.45010	0.40129	0.677
		3.00	3.31	-0.23308	0.39342	0.934

Table 5—Continued.

HCEMAIL	1.00	2.00	3.67	-1.05068*	0.32150	0.007**
		3.00	3.46	-0.83500*	0.31110	0.039*
		4.00	3.38	-0.75962	0.47132	0.374
	2.00	1.00	2.62	1.05068*	0.32150	0.007**
		3.00	3.46	0.21568	0.20987	0.733
		4.00	3.38	0.29106	0.41159	0.894
	3.00	1.00	2.62	0.83500*	0.31110	0.039*
		2.00	3.67	-0.21568	0.20987	0.733
		4.00	3.38	0.07538	0.40352	0.998
	4.00	1.00	2.62	0.75962	0.47132	0.374
		2.00	3.67	-0.29106	0.41159	0.894
		3.00	3.46	-0.07538	0.40352	0.998
HCLICENS	1.00	2.00	4.00	-1.12500*	0.27969	0.001***
		3.00	4.05	-1.17500*	0.27019	0.001***
		4.00	4.15	-1.27885*	0.40934	0.011*
	2.00	1.00	2.87	1.12500*	0.27969	0.001***
		3.00	4.05	-0.05000	0.18299	0.993
		4.00	4.15	-0.15385	0.35783	0.973
	3.00	1.00	2.87	1.17500*	0.27019	0.001***
		2.00	4.00	0.05000	0.18299	0.993
		4.00	4.15	-0.10385	0.35045	0.991
	4.00	1.00	2.87	1.27885*	0.40934	0.011*
		2.00	4.00	0.15385	0.35783	0.973
		3.00	4.05	0.10385	0.35045	0.991
HCVEHICL	1.00	2.00	4.52	-0.68721*	0.21825	0.010**
		3.00	4.53	-0.69667*	0.21083	0.006**
		4.00	4.69	-0.85897*	0.31942	0.039*
	2.00	1.00	3.83	0.68721*	0.21825	0.010**
		3.00	4.53	-0.00945	0.14279	1.000
		4.00	4.69	-0.17176	0.27922	0.927
	3.00	1.00	3.83	0.69667*	0.21083	0.006**
		2.00	4.52	0.00945	0.14279	1.000
		4.00	4.69	-0.16231	0.27347	0.934
	4.00	1.00	3.83	0.85897*	0.31942	0.039*
		2.00	4.52	0.17176	0.27922	0.927
		3.00	4.53	0.16231	0.27347	0.934
HCWEB	1.00	2.00	4.35	-0.68468*	0.25100	0.035*
		3.00	4.25	-0.58844	0.24335	0.077
		4.00	4.46	-0.79487	0.36796	0.138
	2.00	1.00	3.66	0.68468*	0.25100	0.035*
		3.00	4.25	0.09635	0.16456	0.937
		4.00	4.46	-0.11019	0.32133	0.986
	3.00	1.00	3.66	0.58844	0.24335	0.077
		2.00	4.35	-0.09625	0.16456	0.937

Table 5—Continued.

		4.00	4.46	-0.20644	0.31540	0.914
	4.00	1.00	3.66	0.79487	0.36796	0.138
		2.00	4.35	0.11019	0.32133	0.986
		3.00	4.25	0.20644	0.31540	0.914
HCPHOTO	1.00	2.00	3.52	-1.13572*	0.30328	0.001***
		3.00	3.13	-0.73870	0.29378	0.061
		4.00	3.53	-1.14716*	0.44081	0.048*
	2.00	1.00	2.39	1.13572*	0.30328	0.001***
		3.00	3.13	0.39703	0.19480	0.177
		4.00	3.53	-0.01143	0.38204	1.000
	3.00	1.00	2.39	0.73870	0.29378	0.061
		2.00	3.52	-0.39703	0.19480	0.177
		4.00	3.53	-0.40846	0.37455	0.696
	4.00	1.00	2.39	1.14716*	0.44081	0.048*
		2.00	3.52	0.01143	0.38204	1.000
		3.00	3.13	0.40846	0.37455	0.696

* $p < .05$. ** $p < .01$. *** $p < .001$.

Hypothesis 2: There is no difference between gender categories in determining what Protected Health Information is desired to protect from a healthcare provider. The hypothesis question was answered by analyzing survey Question 9 (“What is your gender?”), Question 2 (“Do you believe that your healthcare team, those caring for you when you are in a care facility, should be able to see the following information?”).

A One-Way Analysis of Variance was used to test for significant differences among the gender groups and each Protected Health Information indicator. There was a significant difference between males and females, utilizing a significance level of .05 for their opinion on whether the healthcare team should be able to see PHI on name of relatives ($p < .037$). Males ($M=2.57$, $SD=1.17$) indicated a desire for more privacy in regard to the sharing of their relatives’ names with healthcare providers than females

($M=2.23$, $SD=1.17$). Therefore, Null Hypothesis 3 was rejected for relative and retained for the other 16 Protected Health Information indicators. These data are summarized in Table 6.

Table 6

ANOVA for Hypothesis 2—Gender

PHI	Male		Female		<i>df</i>	<i>F</i>	<i>p</i>
	<i>M</i>	<i>SD</i>	<i>M</i>	<i>SD</i>			
Name	1.13	0.47	1.19	0.66	1,209	0.606	.430
Address	2.40	1.32	2.38	1.37	1,209	0.006	.940
Relative	2.57	1.17	2.23	1.17	1,208	4.400	.030*
Employer	3.29	1.18	3.16	1.34	1,208	0.514	.474
Birth Date	1.63	0.98	1.61	0.93	1,208	0.040	.842
Telephone	2.41	1.32	2.37	1.36	1,207	0.053	.819
Fax	3.37	1.37	3.07	1.40	1,209	2.350	.127
Email	3.53	1.31	3.32	1.47	1,209	1.190	.276
SSN	3.49	1.36	3.18	1.48	1,209	2.370	.125
MRN	1.76	1.04	1.68	0.99	1,208	0.307	.580
HPN	2.25	1.27	2.07	1.23	1,209	1.030	.311
Acct. No.	2.18	1.33	2.11	1.29	1,205	0.151	.698
License No.	3.97	1.20	3.83	1.27	1,208	0.677	.411
Vehicle No.	4.50	0.92	4.41	0.97	1,208	0.470	.494
Web Address	4.30	1.03	4.16	1.13	1,207	0.907	.342
Finger/Voice	3.92	1.24	4.08	1.22	1,208	0.802	.371
Photo Images	3.15	1.33	3.27	1.28	1,208	0.450	.503

Note. $N=207-211$. SSN= Social Security number; MRN= medical record number; HPN= health plan number.

* $p<.05$.

Research Question 3

The third major research question in this study was, What is the relationship between authority ascribed to physicians and who has access to healthcare information?

In developing appropriate hypothesis statements related to Question 3, there exist two independent variables: age and authority. The dependent variables are: Insurance Provider, Spouse, Parent, Significant Other, Child, Siblings, Doctor, Nurse, Therapist, Researcher, Law Enforcement, Pharmacist, Pastor (religious advisor). To address this research question, the following three hypotheses were tested:

Hypothesis 3: There is no difference among patients who ascribe various levels of authority to their physicians and their comfort level with other people having access to their healthcare information. The hypothesis was tested by analyzing responses to survey Question 1 ("Do you believe that your doctor has the ultimate authority when it comes to your healthcare?") and Question 5 ("How comfortable are you with the following persons having access to your health information?").

Hypothesis 4: There is no difference between younger and older patients regarding their comfort level with other people having access to their healthcare information. The hypothesis question was answered by analyzing responses to survey Question 5 ("How comfortable are you with the following persons having access to your health information?") and Question 8 (What is your present age?).

Hypothesis 5: There is no interaction between patients who ascribe various levels of authority to their doctor and the age of the patient regarding their comfort level with other people having access to their healthcare information. The hypothesis question was answered by analyzing responses to survey Question 1 ("Do you believe that your doctor

has the ultimate authority when it comes to your healthcare?"), Question 5 ("How comfortable are you with the following persons having access to your health information?") and Question 8 (What is your present age?").

Two-Way Analysis of Variance was used to determine the main effect and interaction effect of age and authority on access of health information by insurance provider, spouse, parent, significant other, child, siblings, doctor, nurse, therapist, researcher, law enforcement, pharmacist, and pastor (religious advisor). Subjects were divided into four age groups (Group 1: 18-30; Group 2: 31-45; Group 3: 46-60; Group 4: 61-70). In order to protect the assumptions underlying the analysis of variance, age groups were combined for analysis on all independent variables. New age groups were Group 1: 18-45, and Group 2: 46-70.

Participants were asked to score their belief on what degree they believed their doctor has ultimate authority when it comes to their healthcare utilizing the 5-point Likert Scale of measurement. Participants were then asked to score their comfort level with giving access to health information. In order to protect the assumptions underlying the analysis of variance, results of the scoring were combined into three groups for all independent variables (Group 1: "always" and "mostly," Group 2: "sometimes," Group 3: "almost never" and "never"). For purposes of this analysis, the following criteria were used to determine the degree of access on healthcare information by the 13 dependent variables. If the overall mean scores ranged from 1.00-2.33, then access of healthcare information is "always" accessible. If the mean score was 2.34-3.67, healthcare information is "sometimes" accessible, and if mean scores fell between 3.68 and 5.00, healthcare information should "never" be accessible by the identified dependant variable.

Table 7 shows the overall mean score for each dependant variable. Higher mean scores indicate more desire for privacy. Access of healthcare information was "always" allowed by the respondent for most of the dependent variables. The exceptions were parent, significant other, child, sibling, researcher, and pharmacist, for which these dependent variables were "sometimes" allowed access to information. Law enforcement and pastor were "never" allowed access to healthcare information. These data are summarized in Table 7.

Table 7

Mean Score—Healthcare Information Access

<i>Variable</i>	<i>Mean</i>	<i>SD</i>
Insurance	2.31	0.937
Spouse	1.79	1.090
Parent	2.43	1.200
Significant Other	2.49	1.270
Child	2.82	1.170
Sibling	2.86	1.170
Doctor	1.31	0.600
Nurse	1.78	0.977
Therapist	1.99	1.070
Researcher	3.36	1.110
Law	3.93	0.975
Pharmacist	2.53	1.080
Pastor	3.74	1.150

Note. N=187-208.

There was a statistically significant main effect for authority given to doctors and access of healthcare information by significant other ($p < .033$), child ($p < .045$), law enforcement ($p < .001$), and pastor (religious advisor) ($p < .001$). These data are summarized in Table 8.

Table 8

ANOVA for Hypothesis 3—Access by Individuals to Healthcare Information Based on Authority Given to Doctor

Access to Information	Always		Sometimes		Never		df	F	p
	M	SD	M	SD	M	SD			
Insurance	2.29	0.874	2.26	0.899	2.37	1.020	2,195	0.377	.687
Spouse	1.64	1.000	1.88	1.060	1.89	1.180	2,198	1.440	.238
Parent	2.28	1.190	2.46	1.160	2.56	1.230	2,200	1.180	.309
Significant Other	2.18	1.180	2.68	1.250	2.68	1.320	2,181	3.460	.033*
Child	2.58	1.200	2.88	1.080	3.02	1.150	2,196	3.140	.045*
Sibling	2.68	1.250	2.90	1.060	3.02	1.150	2,198	1.810	.165
Doctor	1.29	0.623	1.30	0.540	1.34	0.622	2,202	0.284	.753
Nurse	1.72	0.973	1.76	0.899	1.86	1.030	2,201	0.656	.520
Therapist	1.92	1.080	2.00	1.040	2.05	1.090	2,199	0.375	.688
Researcher	3.16	1.140	3.37	0.915	3.57	1.180	2,196	2.920	.056
Law	3.73	1.050	3.78	1.030	4.25	0.741	2,199	6.730	.001***
Pharmacist	2.41	0.994	2.38	1.120	2.75	1.130	2,201	2.780	.064
Pastor	3.34	1.240	3.92	1.090	4.03	0.985	2,200	9.200	.001***

Note. Group 1 = Always and mostly, Group 2 = sometimes, Group 3 = almost never and never; $N=187-208$.

* $p < .05$. ** $p < .01$. *** $p < .001$.

Post-hoc comparisons using the Tukey HSD test for “significant other” indicated the mean score for authority given to doctors as “always” and “mostly” ($M=2.18$, $SD=1.18$) was significantly different from the authority given “sometimes” ($M=2.68$, $SD=1.25$) and “almost never” and “never” ($M=2.68$, $SD=1.32$). Those who always and mostly give ultimate authority to their doctors when it comes to healthcare are more willing to give access to healthcare information to their significant other than those individuals who sometimes, almost never, and never give ultimate authority to their doctors on healthcare.

The Tukey test means do not show significance ($p=.074$); however, ANOVA indicates there is a difference between the means at the .05 level, and therefore it is close to being significant since Tukey has less power than Two-Way ANOVA. I will interpret the significance with ANOVA; therefore, the groups are considered to be significantly different. Table 9 displays data for significant other.

Table 9

Tukey HSD Test With Significance of .01—Significant Other

Authority Score	<i>N</i>	Subset 1
Always and Mostly	71	2.18
Sometimes	47	2.68
Almost Never and Never	69	2.68
Sig.		.074

Note. Means for groups in homogeneous subsets are displayed. Based on Type III Sum of Squares. The error term is Mean Square (Error) = 1.542. (a) Uses Harmonic Mean Sample Size = 60.176. (b) The group sizes are unequal. The harmonic mean of the group sizes is used. Type I error levels are not guaranteed. (c) Alpha = .01.

Post-hoc comparison for the independent variable of child does not show a significant difference between the groups. Table 10 displays data for child.

Post-hoc comparisons for law enforcement show group 1, “always” and “mostly” ($M=3.73$, $SD=1.05$) different from group 3, “almost never” and “never” ($M=4.25$, $SD=0.741$). Group 3 also is significantly different from group 2, the group that “sometimes” ($M=3.78$, $SD=1.03$) gives authority to their doctors. Those who “almost always” give doctors authority as their healthcare provider differ from those who “almost never” give authority on how they feel about access of healthcare information by law enforcement. Group 1, who always gives authority to their doctor, is more likely to give access to law enforcement on their healthcare information than group 3. Group 3, those who “almost never” give authority to their doctor, is less likely to want law enforcement having access to their healthcare information than group 2, who sometimes gives authority. Although there is a difference between the groups, all groups desired privacy and want to limit access of healthcare information to law enforcement. Table 11 displays data for law enforcement.

The post-hoc comparisons for pastor show group 1, “always” and “mostly” ($M=3.34$, $SD=1.24$), differs significantly from group 2, “sometimes” ($M=3.92$, $SD=1.09$), and group 3, “almost never” and “never” ($M=4.03$, $SD=0.98$), in their willingness to give access to their pastor or religious advisor. Those respondents who “always” give authority to their doctor are more likely to give access to healthcare information to their pastors or religious advisors than those who “sometimes” or “almost never” give authority to their doctors. Table 12 displays data for pastor (religious advisor).

Table 10

Tukey HSD Test With Significance of .01—Child

Authority Score	<i>N</i>	Subset
Always and Mostly	77	2.58
Sometimes	51	2.88
Almost Never and Never	74	3.02
Sig.		.076

Note. Means for groups in homogeneous subsets are displayed. Based on Type III Sum of Squares. The error term is Mean Square (Error) = 1.335. (a) Uses Harmonic Mean Sample Size = 65.064. (b) The group sizes are unequal. The harmonic mean of the group sizes is used. Type I error levels are not guaranteed. (c) Alpha = .01.

Table 11

Tukey HSD Test With Significance of .01—Law Enforcement

Authority Score	<i>N</i>	Subset	Subset
Always and Mostly	79	3.73	
Sometimes	52	3.78	3.78
Almost Never and Never	74		4.25
Sig.		.942	.014

Note. Means for groups in homogeneous subsets are displayed. Based on Type III Sum of Squares. The error term is Mean Square (Error) = 0.904. (a) Uses Harmonic Mean Sample Size = 66.076. (b) The group sizes are unequal. The harmonic mean of the group sizes is used. Type I error levels are not guaranteed. (c) Alpha = .01.

Table 12

Tukey HSD Test With Significance of .01—Pastor Religious Advisor

Authority Score	<i>N</i>	Subset 1	Subset 2
Always and Mostly	79	3.340	
Sometimes	51		3.920
Almost Never and Never	76		4.030
Sig.		1.000	.813

Note. Means for groups in homogeneous subsets are displayed. Based on Type III Sum of Squares. The error term is Mean Square (Error) = 1.220. (a) Uses Harmonic Mean Sample Size = 66.044. (b) The group sizes are unequal. The harmonic mean of the group sizes is used. Type I error levels are not guaranteed. (c) Alpha = .01.

The Tukey test means do not show significance ($p=.813$); however, ANOVA indicates there is a difference between the means at the .05 level but not at the .01 level, and it is close to being significant since Tukey has less power than Two-Way ANOVA. I will interpret the significance with ANOVA; therefore, the groups are interpreted as being significantly different.

No significant difference was found by authority given to doctors and healthcare access for insurance provider, spouse, parent, siblings, doctor, nurse, therapist, researcher, and pharmacist. Therefore hypothesis 3, there is no difference among levels of authority on healthcare information access, is retained for these but rejected for significant other, child, law enforcement, and pastor.

In response to hypothesis 4, data in Table 13 show there was a statistically significant main effect for age and access of healthcare information. Two age groups, group 1 (18-45) and group 2 (46-70), show a difference in their willingness to grant

access to healthcare information. The younger group is more private with access to their healthcare information when it comes to insurance providers ($p < .046$), spouse ($p < .036$), significant other ($p < .049$), and pastor (religious advisor) ($p < .006$), therefore hypothesis 4 was rejected for these variables.

No significant differences were found by age and access of healthcare information for parent, child, sibling, doctor, nurse, therapist, researcher, law enforcement, or pharmacist. Therefore hypothesis 4 was retained for these variables.

Table 13

ANOVA for Hypothesis 4—Age Groups and Healthcare Access

Access to Information	Ages 18-45		Ages 46-70		df	F	p
	M	SD	M	SD			
Insurance	2.46	1.020	2.18	0.833	1,195	4.030	.046*
Spouse	1.96	1.240	1.64	0.918	1,198	4.450	.036*
Parent	2.50	1.340	2.37	1.060	1,200	0.419	.518
Significant Other	2.70	1.360	2.29	1.150	1,181	3.910	.049*
Child	2.97	1.210	2.68	1.120	1,196	3.010	.084*
Sibling	2.96	1.280	2.76	1.060	1,198	1.280	.259
Doctor	1.40	0.715	1.22	0.462	1,202	3.350	.069
Nurse	1.83	1.060	1.74	0.896	1,201	0.217	.642
Therapist	1.97	1.060	2.00	1.090	1,199	0.158	.691
Researcher	3.45	1.020	3.28	1.190	1,196	1.260	.262
Law	4.03	0.918	3.85	1.020	1,199	2.060	.152
Pharmacist	2.58	1.130	2.48	1.040	1,201	0.340	.561
Pastor	3.95	1.130	3.54	1.140	1,200	7.790	.006**

Note. $N=187-208$.

* $p < .05$. ** $p < .01$.

There was no interaction between authority and age in regard to healthcare information access, therefore, hypothesis 5 was retained. Table 14 displays data for interaction between authority level granted and age.

Research Question 4

The fourth research question considered within the study was, What is the level of financial commitment given by the patient to protect each Protected Health Information mandated by the privacy rule?

Table 14

ANOVA for Hypothesis 5—Interaction Between Authority and Age Regarding Access

Access to Information	Type III Sum of Sq.	Mean Square	df	F	p
Insurance	0.369	0.184	2,195	0.211	.810
Spouse	0.305	0.152	2,198	0.130	.878
Parent	1.690	0.847	2,200	0.583	.559
Significant Other	3.030	1.510	2,181	0.985	.376
Child	1.410	0.706	2,196	0.529	.590
Sibling	1.440	0.720	2,198	0.521	.595
Doctor	1.360	0.683	2,202	1.920	.148
Nurse	5.220	2.610	2,201	2.760	.065
Therapist	5.740	2.870	2,199	2.480	.086
Researcher	2.320	1.160	2,196	0.947	.390
Law	0.233	0.117	2,199	0.129	.879
Pharmacist	2.530	1.260	2,201	1.080	.340
Pastor	0.066	0.033	2,200	0.027	.973

Note. N=187-208.

* $p < .05$.

On the original survey, participants were asked to give each Protected Health Information a monetary value using an industry standard for dollar value for how much they would invest to protect their privacy. For the survey question number 6 (“How much of your own money would you invest in protecting the privacy of the Protected Health Information?”) the scale utilized was 1=*Low*; 2=*Medium*; 3=*High*. For the purpose of this analysis, a frequency distribution was used to establish the rating of each PHI based on dollar value given. Mean values between 1–1.66 were considered “low value”; values between 1.67–2.33 are “medium value”; and 2.34–3.00 carried “high value” for what the participant was willing to spend to protect the privacy of the Protected Health Information. The top four positions on mean value were Social Security number (2.20), finger/voice (1.98), medical record number (1.84), and photo images (1.81). The indicators carrying the lowest scores include, name (1.33), employer (1.42), birth date (1.47), and web address/IP address (1.48). None of the Protected Health Information indicators scored a “high value.” Data in Table 15 show the frequencies ranked as well as mean value for all Protected Health Information indicators.

Research Question 5

The fifth research question within the study was, What other information do the respondents think should be kept private?

An open-ended question at the conclusion of the study asked each respondent to list any other information they think should be kept private. A free-form text box was provided. In order to analyze this question, I organized each response into thematic categories. These categories consisted of the following: Category 1: Financial, consisting of financial income, credit card information, and checking account information. Category

2: Medical, includes responses on medical diagnosis, drug history, and psychosocial history. Category 3: Other, includes those items that did not fall within the financial and medical categories. Free-text statements in the thematic categories are represented here.

Table 15

Frequency Distribution for Dollar Value on Each PHI

PHI	Low (\$) <i>f</i>	Medium (\$\$) <i>f</i>	High (\$\$\$) <i>f</i>	Overall Mean Score
SSN	56	51	98	2.20
Finger/Voice	69	68	66	1.98
MRN	85	65	53	1.84
Photo Images	83	72	46	1.81
License No.	96	68	40	1.72
HPN	98	69	36	1.69
Acct. No.	101	66	36	1.67
Vehicle No.	103	62	38	1.67
Email	99	76	28	1.65
Telephone	100	76	27	1.64
Relative	113	69	21	1.54
Fax	113	70	21	1.54
Address	124	61	19	1.48
Web Address	125	57	21	1.48
Birth Date	130	52	22	1.47
Employer	134	52	17	1.42
Name	151	36	16	1.33

Note. SSN= Social Security number; MRN= medical record number; HPN= health plan number.

Category 1, financial information, contained comments related to the desire to keep financial information private. Twenty-one entries were included within the free-text section of the survey. Participants include such comments as, "I think credit card information, account balances, financial income, and annual income should be kept private or any other information that can be used against you." Financial income, credit card data, and checking account information were among the top most reported financial information to keep private.

Category 2, medical information, contained 38 specific comments related to medical diagnosis, physical history, psychosocial history, lab results, and genetic profile. Additional comments were included that addressed in particular the process regarding how privacy should be deployed among healthcare providers. These comments included, "I feel healthcare needs to correct some very simple privacy issues. For example, calling out names in a doctor's office. Front desk employees using patient information when ordering medication and lab tests on phones that are in hearing distance of the waiting room." "Doctors and nurses should not discuss a patient diagnosis, illness, obesity, or any patient-related topic in locations frequented by guest, visitors, or family members." "Psychosocial information, drug or alcohol use, sexual history should not be discussed openly." "Personal information should only be accessed on a need-to-know basis with full consent of patient." "I think that when you're in the hospital, sometimes the nurses come in and start talking about your medical condition and ask all kinds of personal questions when your visitors are in the room. I think that if they need to direct you to do something or ask you about your condition they should not do it in front of your visitors."

For Category 3, Other, of the free-text comments that were collected, there were 12 valuable comments that fell outside the category of financial and medical. These have been listed within the "other" category, and contain such comments related to treatment based on golden rule, paying for privacy, ethnic background, religion, and sexual history. A collection of these comments includes: "With the age of technology there are several ways to do things that are immoral, illegal and down right nasty. However it should be noted that earthly life is finite and will end and the ultimate responsibility is with the individual and where they choose to spend eternity. I hope your survey goes well and that most people follow the golden rule." "I shouldn't have to pay a dime to keep my medical information private. New HIPAA regulations require the information be kept confidential." "I shouldn't have to pay anything to keep my information private." "Almost any information the government uses for social engineering such as ethnicity, sexual preference, salary, value of home, and use of personal vehicle."

The collection of free-text comments allowed participants to self-express their concerns over what additional information should be kept private outside of the PHI indicators. This information can be of value as the HIPAA regulation is considered for revision in the future.

Chapter 5 includes a summary of these results and provides conclusions and recommendations.

CHAPTER FIVE

SUMMARY, CONCLUSIONS, AND RECOMMENDATIONS

The purpose of this study was to survey a selected population of healthcare consumers (patients) to identify their perspectives on certain personal privacy issues related to the HIPAA Protected Health Information (PHI) indicators. The study focused on four key areas: (a) the type of information the consumer wants to keep private; (b) the relationship of age, gender, and authority level in the desire for privacy; (c) who should access information; and (d) the economical priority given to protecting each PHI indicator.

Theoretical Basis for the Study

Personal privacy has been described as “the most comprehensive of rights and the most valued by civilized men” (*Olmstead v. United States*, 1928, p. 438). The term privacy has been defined in many different ways. Some assert that privacy is the “right of the individual to determine when, how, and to what extent there should be a disclosure of information about himself” (AEI Legislative Analyses, 1997). Others say privacy can be seen “as creating the context in which both deceit and hypocrisy may flourish” (Schoeman, 1984, p. 1). Therefore the opening up of society and creating a transparent view would encourage accountability and build safer communities.

Transparency of information means *all* of society is under the same scrutiny and surveillance, and that no one is exempt. Brin (1998) suggests that when transparency is

reciprocal and people retain a sense of self-control, distrust and fatalism do not exist. Transparency brings about accountability, and it changes the consciousness of human behavior. Therefore individual rights can be respected and less governmental control is needed to control the deceit and wrongdoings of the few, thus honoring the privacy of the individual and giving him greater freedom to act as he wills.

Transparency is directly related to accountability. Brettschneider (2002) addresses mutual justification as a means of defending privacy, property, welfare, and life. Quoting M. N. Plano, Brin (1998) sums up privacy in our current society:

We are entering the age of mirages, illusions, and make believe. While some people are blinded by all pervading noise, others acquire X-ray eyes, letting them see beyond all the old, traditional walls. For a while, this will create a golden time of opportunity for swindlers, blackmailers, and all kinds of cheaters. But then we will adapt. (Brin, 1998, p. 262)

The concept of transparency is practiced within healthcare. Patients render information in order to receive care for an illness. The accountability to provide accurate information to one's healthcare provider is directly related to the treatment plan delivered. Fraud and deceit are shortly discovered through invasive techniques and information provided through technology; truth is rendered by cause and affect.

A key component of the American healthcare system is the ability to exchange private healthcare information to create a medical record comprehensive enough to treat the illness, recover charges incurred, and gather enough data to build the knowledge needed for research to better improve patient care.

As clinicians and other healthcare professionals began to utilize technology to make care decisions, conduct research, manage patient visits, and manage patient reimbursement, public interest over providing privacy and security of healthcare data is a

growing concern. The government responded to these concerns by extending the Health Insurance Portability Accountability Act 1996 (HIPAA) to include privacy and security of patient data under the HIPAA regulation (Kennedy-Kassebaum, 1996).

Most individuals who grant authority to healthcare providers trust the reputation and competency of healthcare professionals. They are willing to be "transparent" and to allow their personal information to be in the hands of their healthcare providers (Louis Harris and Associates, 1993). Transparency of certain personal information about a society's citizens is vital to its infrastructure. In order for social systems to survive and grow, a degree of transparency about personal information is critical.

David Brin (1998) believes that "the flow of information is the flow of life" (p. 333). Transparency is not about forgoing privacy, but about giving society the power to hold accountable those who would violate privacy. Brin states that those who want to do harm have far more freedom to do so in a world of secrecy than in a world of light.

Esther Dyson (as quoted in Brin, 1998) stated, "The challenge is not to keep everything secret, but to limit misuse of information. That implies trust, and more information about how the information is used. At the same time we may all become tolerant if everyone's flaws are more visible" (p. 310).

Relinquishing private information has been identified in anthropological data as particular to enculturation (Gray-Lukkarila, 1997). In American culture, we tend to protect personal privacy in order to maintain our image of personal self (Gray-Lukkarila, 1997).

Tal Yuval (1997) has defined how privacy and social norms have a causal connection to individual behavior. The accountability brought about by social

transparency may be necessary for individuals to thrive socially, economically, and politically. Notice the words of Peter Schwartz and Peter Leyden (1997), commentators of the magazine *Wired*:

With the coming of *Wired*, global society, the concept of openness has never been more important. It's the linchpin that will make the new world work, in a nutshell; the key formula for the coming age is this: Open, good. Closed, bad. Tattoo it on your forehead. Apply it to technology standards, to business strategies, to philosophies of life. It's the winning concept for individuals, for nations, for the global community in years ahead. (p. 15)

A person who enjoys privacy is said to have the ability to control whom they choose to release information to, and to whom they choose to keep information from (Fried, 1968). Yet to mandate who can give and receive information supports the concept of private sanctuaries that hold and restrict the individual.

Historically the American healthcare industry has constructed a culturally, politically, and socially open infrastructure based on the reputation of healthcare professionals to keep information private. This information is used to render care, conduct research to improve health for our communities, provide payment for services rendered, and to protect society (protection from epidemics, etc.). Healthcare Transparency simply continues the same principles of openness as a way of increasing economic stability, expanding the knowledge base through clinical research, and bringing about the efficiency of healthcare delivery that will ultimately improve human well-being and provide the greatest good for the greatest number.

Related Literature

The literature review is divided into four key areas: First, the origin of privacy as related to culture and personal identity. Second, the key judicial cases that support the

idea of privacy within society. Third, healthcare privacy issues (including some key judicial cases around health law). And fourth, the transparent side of privacy issues, and the discrepancies that exist between expressed privacy concerns and individual responses to procuring privacy within society.

Privacy emerged as a value within our culture, and recognition of the desire for privacy grew as our social structure became more advanced and the threat of personal autonomy grew. Thomas Hobbes (1651) supported strong governmental controls to restrict personal autonomy, thereby building a foundation of political infrastructure that could put requirements on society to live and act within the imposed boundaries set forth by the political leaders.

John Locke (1690) believed people by nature had a right to liberty. Locke refuted Hobbes's belief that the only way to bring harmony and comfort to mankind was through an ultimate authority. Instead Locke defined the ideal relationship between a state and its citizens as a contractual one—a constitutional government with a clear separation of powers between the legislative, executive, and judiciary branches.

In *The Social Contract* (1762), Rousseau wrote, "Man was born free, and he is everywhere in chains" (p. 1). His social contract theory states that the legitimacy of the state is based on the agreement of individual human beings to surrender some or all of their private rights in order to secure the protection and stability of an effective social organization or government.

America's founding fathers also understood that one's personal possessions brought status and social ranking. The scrutiny by society could cause one's personal space to be imposed upon, leading to the need for protection of personal property. In

1791, the Bill of Rights guaranteed that one's possessions were protected. However, the Constitution took no direct stand regarding privacy between individuals. Although the United States Constitution does not mention the word "privacy," certain privacy rights are implied in the Bill of Rights (1791) and other amendments that followed the Bill of Rights. Sections of the Bill of Rights that pertain to privacy include the First Amendment (freedom of religion and expression), the Fourth Amendment (freedom from unreasonable search and seizure), the Fifth Amendment (no legal duty to incriminate oneself), and the Ninth Amendment (implied rights not enumerated). Throughout the 20th century, the courts increasingly dealt with cases related to personal liberties and privacy rights. Questions were continually raised about how much the United States Constitution supported the right to individual privacy.

The expansion of social demands for the recognition of privacy grew out of ongoing social, political, and economic changes. In the 19th century, protection was given only for interference with life and physical property. The publication of "The Right to Privacy" (Warren & Brandeis, 1890) resulted in public recognition of the right to have a private life. In 1905, the Supreme Court of Georgia became the first court to recognize what is now referred to as "right to privacy" in an advertisement case against a life insurance company (*Pavesich v. New England Life Insurance Co.*, 1905).

The case of *N.A.A.C.P. v. Alabama* (1958) provided a legal basis supporting the concept that an individual's name is a protected property. This landmark ruling supports the idea that a person's name is a "protected" piece of information owned by the individual, and the individual has the right to release or not release the information. The

legal reasoning behind this case is that there is a vital relationship between freedom to associate and one's privacy in associations.

The case of *Griswold v. Connecticut* (1965) extended the concept of privacy to healthcare information. The Executive Director of Planned Parenthood and Medical Director sued the state, claiming the statute violated the Fourteenth Amendment. The court found in favor of the Executive Director of Planned Parenthood and its Medical Director, ruling that the statute violated the Fourteenth Amendment by taking away the individual's freedom to decide conception. It also ruled that it is a person's right to exchange information with their healthcare provider without having that information scrutinized by others. This case was the first time a majority of the court had embraced the concept of patient privacy rights within healthcare. It held that personal privacy in healthcare is protected from government intrusion (*Griswold v. Connecticut*, 1965).

In the case of *Roe v. Wade* (1973), the principal thrust of the court's attack on the Texas statutes is that it improperly took away a personal right, in this case the right of Roe to terminate her pregnancy. Historically *Roe* has attached itself to the concept of a "woman's right to choose." However, it has more to do with the concept of personal autonomy and the role that privacy plays in a society's right to make choices (Alderman & Kennedy, 1995). Privacy is not the general concern in the *Roe* case; in fact, the courts acknowledge that "the right" is not absolute and is subject to "state interest." The state should act in the best interest of society.

Utilitarianism has been said to be the philosophy that underlies the modern welfare state (Bentham, 1995). The strength of the utilitarian concept as it applies to *Roe v. Wade* is in the balance between self-interest and the interests of society and its

consequences. Autonomy of self, development and expression of intellect, and personality are protected by the First Amendment and are absolute, not dependent on state interests. Freedom of choice in regard to marriage, divorce, procreation, contraception, and education are not absolutes and are subject to state powers and compelling state interests.

The Wetterling Act (1999), commonly known as "Megan's Law," provides a modern example of the "Greatest Happiness Principle" discussed by John Stuart Mill (1859). Megan's Law requires that those who have committed sex crimes against children be publicly registered. The registry is available for public review. The initiatives behind this act are that (a) sex offenders pose a high risk of re-offending after release from custody, (b) protecting the public from sex offenders is a primary governmental interest, (c) the privacy interests of persons convicted of sex offenses are less important than the government's interest in public safety, and (d) the release of certain information about sex offenders to public agencies and the general public will assist in protecting public safety (Wetterling Act, 1999).

One justification given for the Wetterling Act is families with children who know that John Doe is a convicted sex offender can avoid Doe and keep him away from potential victims. Because the government cannot watch Doe every minute to make sure he is not molesting a child, it enlists the assistance of the civilian population in doing so, therefore making his whereabouts and activities transparent.

In the case of *Warden v. Hayden* (1967), Justice Douglas stated the opinion that privacy "means the individual should have the freedom to select for himself the time and circumstances when he will share his secrets with others and decide the extent of the

sharing" (p. 324). The Privacy Act of 1974 was enacted to control abuses of record keeping by governmental agencies. It was designed to protect individuals from disclosure of confidential information by the Federal government without written consent from the individual giving the information (1974).

Calvin Davis (1977) conducted a qualitative research project in 1977, specifically investigating the Privacy Act as it pertained to medical information. The research focused on the nature and extent of individual privacy, conditions in which individual access to personal files is granted, the rights an individual has to revise, add, or delete information from the files, and what rights individuals have concerning the dissemination of information in their personal files. Davis (1977) stated the belief of the AMA:

Protection of personal information from the private healthcare sector would interfere with and jeopardize the quality of medical services. Dr. Boyle pointed out that there are specific types of situations where confidential healthcare information should be allowed to be transferred or released without direct patient consent and authorization. (pp. 87-88)

Davis's study (1977) focused on the work of Dr. Catherine Rosen. Dr. Rosen was asked by an ACLU attorney whether mental health patients felt they must comply with requests to sign consent forms in order to receive mental health services. The Rosen Study, as referenced within the Davis study, seems to indicate that consumers (patients) may have the desire to disclose personal information under certain circumstances. The current study seeks to add to the knowledge base determined in the Davis study by exploring more specifically what information patients are willing to share and with whom they are willing to share it, and to examine the correlation (if any) between a consumer's age group and the physician's level of authority when it comes to granting access to healthcare information.

The Patient Self Determination Act of 1990 outlines how the healthcare consumer (patient) has the right to make certain decisions concerning medical care. *Ferguson v. City of Charleston* (2001) implies reevaluation of how informed consent forms are utilized within healthcare entities and what power they carry. Like the Patient Self Determination Act of 1990, the HIPAA privacy component is a legislative attempt to satisfy those who believe that personal information will be threatened by technological advances within healthcare. There is no question that as information technology increases, physical access and transfer of health information becomes easier.

The public concerns about computer threats to personal privacy do not seem to be significant when it comes to healthcare entities. *Healthcare Information Privacy*, a 1993 poll conducted by Louis Harris and Associates for Equifax, Inc., identified only 25% of respondents reporting the belief that their medical records had been improperly exposed (Hendersen, 1999, p. 28). The same study showed that only 34% of health professionals believe records were given to unauthorized persons "somewhat often" (Hendersen, 1999). And while the study reported that 85% of the respondents stated that confidentiality of medical information is an important matter, an even greater number (87%) believed that their healthcare providers were keeping medical information confidential (Louis Harris and Associates, 1993).

Trust appears to be a major factor in determining whether individuals will release information. If trust is high, individuals are more willing to share personal information with commercial entities (Milne & Boza, 1999). Horne and Horne (1997) found that "the greater the trust, the less the concern over privacy" (p. 351).

The Louis Harris poll earlier supported the concept that healthcare entities had developed a reputation for being trusted. The National Research Council (1997) acknowledged that a balance between healthcare information access and the protection of patient information is necessary for healthcare entities to operate effectively. The Gallup organization conducted a study of 1,000 participants from the Medic Alert Foundation and found that 90% of those respondents trusted their physician to keep information private and secure; 66% trusted hospitals; 42% trusted insurance companies, and 35% trusted managed care companies. Seven percent of respondents were willing to store and transmit personal healthcare information via the Internet (Fox & Rainie, 2001).

Lind (2002) states that it is important to separate privacy fears into categories, and not allow one area of privacy abuse to overlap into others. Thus in order to fully understand what is important to the healthcare consumer regarding information privacy, it is imperative to differentiate between public concerns over financial or Internet privacy versus potential privacy issues surrounding healthcare information.

Privacy is an ideal, but the reality is that we live in a connected society, and if you want to enjoy the benefits of that society, be it access to credit or access to information, you have to be willing to share information. If people perceive that they're getting special benefits they're much more willing to sacrifice privacy. (Paul, 2001, pp. 3-4)

Methodology

Using a survey instrument (see Appendix), the participants of the Carnegie Financial Insurance group, an independent insurance firm located in Chicago, Illinois, were asked to indicate their perceptions regarding nine quantitative questions and one open-ended question. Participants were asked to score the first five questions using a 1-5 Likert Scale of measurement. Participants were also asked to give a dollar value for what

they were willing to pay to protect each Protected Health Information (PHI) indicator as one of the research questions. The survey concluded with a "free text" area for additional participant input.

The intention of the study was to draw conclusions on the perspectives of the desire for privacy as related to the Health Insurance Portability Accountability Act (HIPAA) PHI indicators as well as the respondents' concern over access to healthcare information by certain defined individuals. The study focused on four key areas: (a) the type of information the consumer wants to keep private; (b) the relationship of age, gender, and authority level in the desire for privacy; (c) who should access information; and (d) the economical priority given to protecting each PHI indicator.

An initial pilot study was conducted using the developed survey tool. This pilot study was used to test the reliability of the tool and the respondents' comments to the usability of the tool. Participants who responded to the pilot study made additional recommendations for improvement.

Following the evaluation of the pilot study, the revised survey tool was distributed via email to the participants of the Carnegie Financial Insurance group. The initial mailing generated an overall 33% response rate. A reminder email was sent, which increased the overall response rate an additional 2% for a total response rate of 35%. The surveys were electronically entered into SPSS and statistical analysis was conducted.

One-Way and Two-Way Analysis of Variance (ANOVA) was used to test each of the stated hypotheses. This method of analysis determined if differences and interactions exist in the perceptions of the respondents on privacy for each PHI indicator and access

to healthcare information by defined individuals such as insurance provider, spouse, and pastor/religious advisors. Age and gender differences were also analyzed.

Summary of Findings

The study explored the consumer's (patient's) perspective regarding what Protected Health Information (PHI) is important to protect and the perspective of respondents on healthcare information access by defined individuals such as insurance provider, spouse, and pastor/religious advisor. The study focused on five research questions:

1. What components of the Protected Health Information do patients want to keep confidential from their healthcare providers?
2. What is the relationship to demographic factors in desire for privacy?
3. What is the relationship between authority ascribed to physicians and who has access to healthcare information?
4. What is the level of financial commitment given by the patient to protect each element of Protected Health Information mandated by the privacy rule?
5. What other information do the respondents think should be kept private?

To address the first research question, What components of the Protected Health Information do patients want to keep confidential from their healthcare providers and others? a frequency distribution was utilized.

The analysis showed, of the 17 Protected Health Information indicators, only 5 of them were identified as being important to protect from healthcare providers. These include email, license number, vehicle serial number, Web address, and finger/voice print. The remaining PHI—name, address, name of relatives, name of employer, birth

date, telephone number, fax number, social security number, medical record number, health plan number, account number, and photo images—were not identified as PHI indicators to be protected from access by healthcare team members.

It is speculated these five PHI indicators (email, license number, vehicle serial, web address, and finger/voice print) are not considered by the patient as important pieces of information that are critical to healthcare decisions. As healthcare technology expands and virtual (remote) care becomes a norm, there is opportunity for email address to be an important component of the healthcare medical record and freely shared in order to provide efficient, safe, cost-effective healthcare in the future. For the remaining 12 PHI indicators (name, address, relatives, employer, birth date, telephone number, fax number, Social Security number, medical record number, health plan number, account number, photo images), the patients appear to trust their healthcare provider and are willing to openly grant access to this information. Transparency of these PHI to healthcare providers is accepted.

Consumers of health are willing to be transparent and are willing to allow their personal information to be in the hands of their healthcare provider. In healthcare, the greatest happiness for the greatest number means providing continued quality healthcare at cost-effective prices. Healthcare Transparency can be a significant tool in achieving this goal. As Brin (1998) states, "The flow of information is the flow of life" (p. 333). The challenge and focus should be to limit misuse of information, to keep information secure from intrusion and abuse, and not to keep information private.

The second research question, regarding the relationship to demographic factors in desire for privacy, explored the following hypothesis:

Hypothesis 1: There is no difference between age categories in determining what Protected Health Information is desired to protect from a healthcare provider.

Hypothesis 2: There is no difference between gender categories in determining what Protected Health Information is desired to protect from a healthcare provider.

A One-Way Analysis of Variance was used to test for significant differences among the age and gender groups and each Protected Health Information indicator. Upon analysis of the data as related to what level of privacy each respondent gave according to their age for each PHI, the data showed significance for the age group 31-45. This group desired more privacy than any other group on name of relative, name of employer, birth date, telephone number, fax number, email, Social Security number, medical record number, and health plan number. The age group 61-70 desired more privacy for license number, vehicle serial number, web address, and photo images. The age group 18-30 scored the lowest on privacy concerns for each PHI indicator than any other group.

Gender differences did exist on the desire for privacy between each PHI; however, there was only significance on 1 of the PHI indicators: Males desired more privacy on name of relative than did females.

The younger age group (18-30) appears to be more willing to adopt transparency. Perhaps this age group growing up with Internet banking, Face Book, online chat rooms, and virtual relationships sees a value in transparency. It is estimated this age group will require more of daily life to be automated, including healthcare. This would include self-scheduling for health services, online health assessments, online medical treatment for minor illnesses, and online access to their medical record. Transparency within the

healthcare setting will be required in order to meet the consumer's (patient's) need for convenience within healthcare services.

The third research question, What is the relationship to physician authority and who has access to healthcare information? analyzed three hypotheses:

Hypothesis 3: There is no difference among patients who ascribe various levels of authority to their physicians and their comfort level with other people having access to their healthcare information.

Hypothesis 4: There is no difference between younger and older patients regarding their comfort level with other people having access to their healthcare information.

Hypothesis 5: There is no interaction between patients who ascribe various levels of authority to their doctor and the age of the patient regarding their comfort level with other people having access to their healthcare information.

Two-Way Analysis of Variance was used to determine the main effect and interaction effect of age and authority on access of health information by insurance provider, spouse, parent, significant other, child, siblings, doctor, nurse, therapist, researcher, law enforcement, pharmacist, and pastor (religious advisor).

Analysis related to access of healthcare information and its cross relationship to the authority granted to physicians was conducted. It was the assumption that the more authority one gave to a doctor, the more transparent with access to healthcare information. It should be noted these hypotheses were not related to PHI, but rather healthcare information in general. The goal was to expand beyond the focus on PHI and probe deeper into the willingness of the patient to be transparent with all healthcare

information. The findings within the study showed the more authority granted to a doctor, the more likely a patient was willing to give healthcare information to their insurance provider, spouse, parent, significant other, child, sibling, doctor, nurse, therapist, researcher, law enforcement, pharmacist, and pastor/religious advisor.

Significant differences existed between those who always give authority and those who never give authority for significant other, child, law enforcement, and pastor/religious advisor. Those who never give authority to their doctor are less likely to give access of healthcare information to significant other, child, law enforcement, and pastor/religious advisor.

There was no statistically significant interaction between authority and age in regard to healthcare access. The younger age group (18-45) is more private with access of healthcare information than the older age group (46-70). The younger age group is less likely to give access to healthcare information to insurance provider, spouse, significant other, and pastor/religious advisor.

The findings on research question 3 are most interesting. The younger generation, ages 18-30, is more transparent with their healthcare provider, yet are less transparent with access of healthcare information to defined individuals, such as insurance provider, spouse, significant other, and pastor/religious advisor. Age appears to play a role in what healthcare information patients want to keep protected from their healthcare providers and the population.

As the patient population ages, and the baby boomer generation floods the healthcare market, the balance between privacy concerns and access of healthcare information will need to be weighed against the consumer's desire for cost-effective

healthcare, ease of payment for services rendered, and high demand for healthcare services that are transferable (provider to providers based on medical specialty).

The fourth research question explored the financial commitment given to privacy by each participant. The research question asked, What is the level of financial commitment given by the patient to protect each element of Protected Health Information mandated by the privacy rule?

The analysis on financial commitment given by the patient to protect each element of PHI showed that no respondents placed a high dollar value (\$\$\$) on protecting any of the PHI indicators. Those PHI which carried a medium dollar value (\$\$) were Social Security number, finger/voice print, medical record number, and photo images. Respondents of the survey stated they are not willing to pay for protection of the PHI indicators, yet HIPAA is estimated to cost healthcare organizations \$17.5 billion over 10 years (2003–2012) (Withrow, 2007). Although participants are not willing to give a financial commitment to protecting the PHI, the cost for HIPAA compliance will be passed down from provider to patient in other ways, such as hospital services, insurance premiums, physician, and clinic professional fees.

The “trickle effect” causes reduced dollars for research, staffing, treatment coverage, and increased insurance premiums. Although HIPAA is not the “blame all” for healthcare’s financial crisis, it does contribute to the overall increase in healthcare entity expenditures. Mandates such as HIPAA continue to flood the healthcare arena and the financial burden to support these mandates such as HIPAA privacy compliance is passed down to the healthcare consumer. To be compliant with regulatory mandates takes staffing and automation of processes. Healthcare entities struggle with staffing, both

nursing and physician shortages, as well as the struggle to automate both patient care and administrative healthcare processes. Regulatory groups put emphasis on patient safety initiatives, which require access to healthcare information and transparency of data. Patients demand expedient care without redundancy of patient information between providers. Consumers of healthcare want cost-effective outcomes and payment for services without hassle and frustration. To answer the question of staff shortages, management of patient care and compliance with patient safety initiatives, it is imperative to automate both administrative processes and clinical care in one seamless record, sometimes referred to as the electronic medical record (EMR). This requires access of patient information and easy transference of data between providers and ancillary systems.

The final research question, What other information do the respondents think should be kept private? gave each participant the opportunity to write in other information they felt should be kept private. Comments were put in thematic categories. Medical diagnosis ranked the highest for the most often listed, as well as financial income, medical history, and credit card information. The awareness of the public's concern over the desire for privacy of medical diagnosis and medical history could add to public opinion on how the HIPAA privacy PHI indicators could be enhanced.

Overall, the findings within each research question support transparency between patient and healthcare provider. The literature review on transparency and opinions related to how privacy is interpreted is supported by a number of legal cases. The five research questions contained within this study and their related findings support the outcomes of such cases as *Warden v. Hayden* (1967), where the opinion of the court was

that privacy “means the individual should have the freedom to select for himself the time and circumstances when he will share his secrets with others and decide the extent of sharing” (p. 324). The guardian of the medical record that contains the PHI information is the healthcare provider, and its privacy is controlled by healthcare entities. Patients choose to share information among healthcare entities; they are free in their actions. That freedom comes from a trust established with the healthcare entity and the value of a greater good: the good of health treatment and payment for services.

In the study conducted by Davis (1977), the research focused on the nature and extent of individual privacy, conditions in which individual access to personal files is granted, rights related to altering the record and what rights individuals have concerning the dissemination of information to physicians, dentists, medical personal, insurance providers, and medical and research review boards. Dr. Rosen, a participant of the study and Director of Research at Northeast Georgia Community Mental Health Center, conducted a study to see if clients would continue to sign the consent form even if they were told they did not have to submit personal information such as name, Social Security number and diagnosis to the state. If they chose to sign the consent form, this information would be shared with the state. Group A was told they did not have to sign the consent form and would still receive treatment. Group B and C were told the state would receive the personal information and that permission was needed to send. In Group A, 40% signed the consent form, and in Groups B and C, 100% signed. Patients chose to release personal information, such as name and Social Security number to healthcare providers even knowing it would be sent to the state. Transparency was practiced. The current

study shows little change in patients' perspective of what should be kept private and therefore not shared with healthcare entities.

The *Ferguson v. City of Charleston* (2001) case brings forth the question of whether HIPAA is necessary and whether patients are already protected against privacy intrusion and abuse by government actors through the Fourth Amendment. This is a case where the more stringent rule could preempt the lesser ruling. The Fourth Amendment protects the "persons, houses, papers, and effects" against unlawful search and seizure by governmental entities. The violation by governmental entities that unlawfully search and seize a patient's PHI and use that information for harm is held to the Fourth Amendment Bill of Rights standards. The unnecessary "loading" of one law on top of another regulation causes confusion and more governmental intrusion.

Conclusions

Overall, patients put little value in protecting the defined PHI as defined by the HIPAA privacy ruling from healthcare providers and are not willing to pay for privacy protection. Patients practice transparency with healthcare providers for much of the PHI and healthcare information. Of those PHI that showed the highest mean score (meaning a higher desire for privacy), 5 out of the 17 PHI researched were considered important enough to limit access by healthcare providers.

Before the debate ensues to agree or disagree on healthcare transparency, it is wise to first acknowledge that fully exposed, transparent societies could pay a social cost by not protecting healthcare information—the cost of individual expression. Jeremy Bentham (cited in Rosen, 2000) utilized the concept of "Panopticon" a ring-shaped structure with windows on all sides that face out into the quarters of those being

observed. This allows individuals to be under constant surveillance (Brin, 1998). Stanley Ben (2000, as cited in Rosen, 2000) noted that when you know you are being observed, it changes your consciousness. Your actions and words become part of third-party scrutiny, and it inhibits the true self (Rosen, 2000).

The threat of one's self-being exposed limits the freedom of expression and exchange of intimate information. Without some protection of personal information there is no freedom of individual expression. If a patient is to be subjected to constant surveillance without the trust and belief in the members of an institution, we potentially limit individual expression and therefore hinder access and receipt of medical care. However, under the context of trust and belief in the institution and its members, individual expression is not impeded. With the institution of HIPAA privacy standards we jeopardize the relationship between physician, nurse, therapist, and the patient. It can be observed that the HIPAA privacy standards do little to support the relationship between healthcare professional and the patient, and merely impede the relationship due to administrative constraints and costs associated with the regulation.

Can intrusion of one's being actually benefit the person and society as a whole? An example is seen in the London underground, where cameras are currently being placed in subways to monitor the activities of patrons; authorities are looking for individuals who act strangely. One such observation is looking for those individuals who stand idle for long lengths of time even though trains go by; these individuals are being monitored for attempted suicide. Once it is determined that the person is at risk, immediate help is sent to the individual, therefore minimizing suicide attempts and healthcare expense. These types of surveillances are intended for public good (Brooks,

2001), yet many worry about the liberties that are being taken away. Thomas Jefferson warned that there is a price for liberty. The acts of September 11th caused questions as to how important are certain liberties. Since September 11th, more people appear to be willing to forgo privacy concerns in order to feel safer. Likewise, it is the belief of this study that patients are willing to forgo certain liberties with healthcare professionals, and that components of the HIPAA's PHI are not required to be protected among healthcare entities. To summarize the findings of this study, the following are identified:

1. Participants are willing to be transparent with healthcare providers regarding 12 of the 17 PHI indicators. The 12 PHI include name, address, name of relatives, name of employer, birth date, telephone number, fax number, Social Security number, medical record number, health plan number, account number, and photo images.
2. The age group 18-30 is more transparent with PHI than any other age group.
3. The more authority given to physicians, the more transparent participants are with access to healthcare information.
4. Participants are not willing to pay for privacy protection for the 17 PHI indicators.
5. Participants consider medical diagnosis and medical history additional indicators that are important to keep private.

Recommendations for Further Research

This study investigated the healthcare consumer's (patient's) perspectives on certain personal privacy issues related to the HIPAA PHI indicators. The study focused on four key areas: (a) the type of information the consumer wants to keep private; (b) the relationship of age, gender, and authority level in the desire for privacy; (c) who should

access information; (d) and the economical priority given to protecting each PHI indicator.

Based on the results of this study, there are a number of other considerations for further study. The results would help to generalize the findings based on sample size, age, and ethnicity.

1. The sample size should be expanded to include different populations, therefore having a larger more diverse sample size in each age group, which would allow a more accurate generalization of the results to the overall population.

2. The expansion of sample size by geographic location would also be beneficial, thereby collecting data from various places across the United States; this would help provide a more reliable generalization of the results.

3. Ethnicity should also be considered for further study, including the data gathering of different ethnic groups. The results could vary in regard to perspectives on healthcare privacy by different ethnic associations.

4. The inquiry into what additional health information should be protected by age, gender, and ethnicity could help identify whether the HIPAA PHI indicators should be expanded to include additional PHI.

5. Evaluation of quality of care standards and how the HIPAA privacy ruling may or may not have had a factor in the findings should be considered. These findings would help to answer the question whether HIPAA has impeded quality of patient care.

6. Investigation into why people do not want their healthcare information accessed by their pastor (religious advisor) should be considered.

7. A further evaluation of survey question 3 should seek to answer what components of the Protected Health Information patients want to keep confidential from others.

Recommendations for Public Policy

This research has shown that for each PHI indicator, the value placed on protecting the PHI indicator from healthcare providers varies. The oldest age group within the study, those over 45 years of age, put little value in protecting each PHI from their healthcare provider and in general give authority to their physician in regard to their healthcare and give access to healthcare information to key individuals such as spouse, insurance provider, and pastor/religious advisor.

The question is then raised, Is the HIPAA privacy ruling achieving what it set out to do? which is to “provide an opportunity for and to encourage more informed discussions between patients and providers about how Protected Health Information will be used and disclosed within the healthcare system” (Federal Register 65, 2000, p.82,474). The privacy legislation was designed to put additional autonomy in the hands of the patient who is receiving care. Do patients care where their information goes within the healthcare system? This study shows participants are willing to release most PHI indicators to healthcare providers.

The HIPAA ruling has brought out an awareness that was needed among healthcare team members, this awareness being the value of keeping chit-chat within the halls and waiting rooms under control. But has it limited the necessary dialog between healthcare team members, patients, families, and other healthcare entities in providing quality, cost-effective care for patients? The risk is present, and the “trickle effect” to

maintain compliance on HIPAA could indeed impact quality of care. The inability to communicate a family member's treatment plan from one family member to another can alter the outcomes for a patient. It is time to re-evaluate the HIPAA privacy ruling and evaluate whether the value it set out to achieve is indeed meeting the expectation of the consumer.

Do the administrative costs to support HIPAA privacy processes outweigh the value of those dollars being spent elsewhere within the healthcare system, such as research, patient safety initiatives, information technology, and community wellness programs? The HIPAA privacy ruling has cost organizations millions of dollars that could have been spent on clinical research, information system technology to advance the practice of care, patient safety initiatives, and community health programs. This study shows that consumers do not put a high value on protecting all the current PHI indicators, so perhaps it is time for a re-evaluation of the PHI indicators and how and from whom they are being protected. Recommendations to public policy on the HIPAA privacy standard include:

1. *Needs assessment of each PHI indicator.* Should additional indicators be added to the HIPAA PHI indicators that provide more value, such as medical diagnosis or medical history?
2. *Evaluation on what qualifies as a "healthcare entity."* Perhaps healthcare providers should not be mandated to comply with HIPAA privacy standards when relating among themselves.
3. *Evaluation of the value of HIPAA to the patient.* Has HIPAA privacy standards procured patient privacy and what value did the patient receive?

4. *Evaluation of the cost of HIPAA compliance by healthcare entities.* This should be weighed against the value these dollars could bring elsewhere.

5. *Building of a technology infrastructure that protects patient data from intrusion.* This should be done without putting the burden on human processes to do so, therefore allowing transparency among healthcare providers and the enhancement of quality care.

6. *Expand security standards as opposed to privacy standard.* This would allow the individual to practice transparency with the assurance that information will be secure.

Privacy concerns cannot all be lumped together in one didactic discussion. Privacy appears to be a value among financial institutions and our personal private sanctuaries; however, when it comes to practice of privacy between healthcare providers, family members, and insurance providers and the individual seeking care, we practice healthcare transparency. Time will tell when our time of adoption for transparency is, when we will see beyond the private sanctuaries we have created to build responsible accountable societies that strive economically, politically, and humanely. We must remember the human heart is something technology will never reach, and we are at our most frailest moment when we face a healthcare crisis. So we must use technology to open up the airways of healthcare information for all to use, and build technological structures to support accountability, security, and reliability of information that will not just help healthcare technology advance but also allow the human spirit to use all its compassion and competence to accomplish great things. It is my opinion that we seek more security of information, not privacy of information. If we choose to relinquish private information and practice our true freedoms of self-expression with whom we

desire, we seek as human beings to trust our information to be secure. It is critical we separate the needs between security of information and privacy of information.

APPENDIX:
HEALTH PRIVACY SURVEY

Healthcare Privacy Survey

Completion of this survey signifies your consent to participate in the study.

Please complete each question

1. Do you believe that your doctor has the **ultimate** authority when it comes to your healthcare? *Please select one*

<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
-------------------------	-------------------------	-------------------------	-------------------------	-------------------------

2. Do you believe that your **healthcare** team (those caring for you when you are in a care facility) should be able to see the following information:

Please select one answer per row

	Always	Mostly	Sometimes	Almost Never	Never
Name	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
Address	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
Name of relatives	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
Name of employers	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
Birth date	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
Telephone Numbers	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
Fax Numbers	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
Email Address	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
Social Security Number	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
Medical Record Number	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
Health Plan Number	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
Hospital Account Number	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
License (any) Number	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
Vehicle Serial Number	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
Web Address	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5

Finger or voice print	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
Photographic Images	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5

3. Should you be able to **limit** who can view the following information:

Please select one answer per row

	Always	Mostly	Sometimes	Almost Never	Never
Name	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
Address	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
Name of relatives	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
Name of employers	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
Birth date	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
Telephone Numbers	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
Fax Numbers	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
Email Address	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
Social Security Number	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
Medical Record Number	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
Health Plan Number	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
Hospital Account Number	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
License (any) Number	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
Vehicle Serial Number	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
Web Address	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
Finger or voice print	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
Photographic Images	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5

4. Should the following information be **viewable** by your healthcare insurance providers?

Please select one answer per row

If no insurance provider, check this box , proceed to Question 5

	Always	Mostly	Sometimes	Almost Never	Never
Name	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
Address	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
Name of relatives	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
Name of employers	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
Birth date	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
Telephone Numbers	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
Fax Numbers	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
Email Address	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
Social Security Number	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
Medical Record Number	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
Health Plan Number	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
Hospital Account Number	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
License (any) Number	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
Vehicle Serial Number	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
Web Address	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
Finger or voice print	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
Photographic Images	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5

5. How **comfortable** are you with the following persons having access to your Health Information (diagnosis, medications, procedures, etc.):

Please select one answer per row

	Always	Mostly	Sometimes	Almost Never	Never
Insurance Provider	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
Family Member					
• Spouse	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
• Parent	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
• Significant Other	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5

• Child	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
• Siblings	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
Healthcare Provider					
• Doctor	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
• Nurse	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
• Therapist	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
Researcher	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
Law Enforcement (Police)	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
Pharmacist	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5
Pastor (religious advisor)	<input type="radio"/> 1	<input type="radio"/> 2	<input type="radio"/> 3	<input type="radio"/> 4	<input type="radio"/> 5

6. How much of your own **money** would you invest in protecting the privacy of the following?

	Low	Medium	High
Name	<input type="radio"/> \$	<input type="radio"/> \$\$	<input type="radio"/> \$\$\$
Address	<input type="radio"/> \$	<input type="radio"/> \$\$	<input type="radio"/> \$\$\$
Name of relatives	<input type="radio"/> \$	<input type="radio"/> \$\$	<input type="radio"/> \$\$\$
Name of employers	<input type="radio"/> \$	<input type="radio"/> \$\$	<input type="radio"/> \$\$\$
Birth date	<input type="radio"/> \$	<input type="radio"/> \$\$	<input type="radio"/> \$\$\$
Telephone Numbers	<input type="radio"/> \$	<input type="radio"/> \$\$	<input type="radio"/> \$\$\$
Fax Numbers	<input type="radio"/> \$	<input type="radio"/> \$\$	<input type="radio"/> \$\$\$
Email Address	<input type="radio"/> \$	<input type="radio"/> \$\$	<input type="radio"/> \$\$\$
Social Security Number	<input type="radio"/> \$	<input type="radio"/> \$\$	<input type="radio"/> \$\$\$
Medical Record Number	<input type="radio"/> \$	<input type="radio"/> \$\$	<input type="radio"/> \$\$\$
Health Plan Number	<input type="radio"/> \$	<input type="radio"/> \$\$	<input type="radio"/> \$\$\$
Hospital Account Number	<input type="radio"/> \$	<input type="radio"/> \$\$	<input type="radio"/> \$\$\$
License (any) Number	<input type="radio"/> \$	<input type="radio"/> \$\$	<input type="radio"/> \$\$\$
Vehicle Serial Number	<input type="radio"/> \$	<input type="radio"/> \$\$	<input type="radio"/> \$\$\$
Web Address	<input type="radio"/> \$	<input type="radio"/> \$\$	<input type="radio"/> \$\$\$

Finger or voice print	<input type="radio"/> \$	<input type="radio"/> \$\$	<input type="radio"/> \$\$\$
Photographic Images	<input type="radio"/> \$	<input type="radio"/> \$\$	<input type="radio"/> \$\$\$

7. What **other** information do you think you should be kept private? *optional*

▲

▼

8. What is your present age? *Please select one*

- 18 - 30
- 31 - 45
- 46 - 60
- 61 - 70
- 71 - over

9. What is your gender? *Please select one*

- Male
- Female

10. What is your race? *Please select one*

- White / Caucasian
- Hispanic
- Asian
- Black / African American
- Native American
- Other (please specify) _____
- I prefer not to answer this question.

Additional Comments: *optional*

REFERENCE LIST

REFERENCE LIST

- AEI Legislative Analyses. (1997). *Privacy protection proposals* (P. Gray-Lukkarila, Ed. & Trans.). Washington, DC: American Enterprise Institute for Public Policy Research.
- Alderman, E., & Kennedy, C. (1995). *The right to privacy*. New York: Alfred A. Knopf.
- Bartnicki v. Vopper, 532 U.S. 514 (2001).
- Bentham, J. (1995). *The panopticon writings* (M. Bozovi, Trans.). London: Verso. (Original work published 1787)
- Bill of Rights*. (1791). Retrieved November 4, 2005, from <http://www.ourdocuments.gov/doc>
- Blue Cross/Blue Shield. (2002, October 10). *Blue Cross & Blue Shield financial estimates for compliance to the privacy component of the HIPAA regulations*. Retrieved October 10, 2003, from <http://www.bdbhealthissues.com>
- Borgstede-Mason, B. A. (1999). Ethics, privacy, and confidentiality issues related to the application of information technology in health care. *Dissertation Abstract International*, 61 (02), 763. (UMI No. 9962543)
- Bowers v. Hardwick, 478 U.S. 186 (1986).
- Brettschneider, C. L. (2002). *Reciprocity and rights: A democratic theory of privacy, property, welfare and life*. Unpublished doctoral dissertation, Princeton University. Princeton, NJ.
- Brin, D. (1998). *The transparent society*. Reading, MA: Addison-Wesley.
- Brooks, M. (2001, November/December). The new bodyguard. *World Link*, 14, 64-65.
- Bureau of Primary Healthcare. (2000). *Electronic transactions and code set standards*. Retrieved June 2003 from Bureau of Primary Healthcare database.
- Campbell, A. (1956). *Moral dilemmas in healthcare*. London: Churchill Livingstone.

- Common Rule § 164.512 United States agency for international development.* (1991, June). Retrieved September 4, 2003, from http://www.usaid.gov/pop_health/resource/phncomrule.htm
- Community Banker. (2001). Online privacy concerns continue to linger. *Stanford Law Review*, 10, 44-47.
- Connecticut Statute, Conn. Gen. Stat. § 53-32, 54-196 (1958).
- Conner, V. (1999, July/August). Patient confidentiality in the electronic age. *Intravenous Nursing*, 199-202.
- Cross, H. L. (1953). *The people's right to know: Legal access to public recordings and proceedings*. New York: Columbia University Press.
- Davis, C. (1977). *The right to privacy and medical information data banks*. Unpublished doctoral dissertation, University of Southern California, Los Angeles.
- Docteur, E., Suppanz, H., & Woo, J. (2003). *The US health system: An assessment and perspective directions for reform and economics department working papers N. 350*. Retrieved October 5, 2004, from <http://www.oecd.org/eco>
- Duhaime Law Museum. (2002). *The British Magna Carta 1215*. (2002). Retrieved February 8, 2003, from http://www.duhaime.org/Law_museum/uk-magna.htm
- Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-2522 (1986).
- EPA, Toxic Release Inventory Program.* (1988). Retrieved June 21, 2006, from <http://www.epa.gov/tri>
- Equifax Inc. (1992). *Harris-Equifax consumer privacy survey*. Atlanta, GA: Author.
- Fair Credit Reporting Act, 15 U.S.C. § 1681 (1970).
- Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (1974).
- Federal Register 65, Standards for Privacy of Individually Identifiable Health Information, Final Rule, 65 Fed. Reg. 82,462-82,474 (Dec. 28, 2000).
- Federal Register 67, Standards for Privacy of Individually Identifiable Health Information, Proposed Rule, 67 Fed. Reg. 14,775 (Mar. 2002).
- Ferguson v. City of Charleston (99-936), 186 F.3d 469 (4th Cir. 2001).
- Foucault, M. (1979). *Discipline and punish: The birth of the prison*. New York: Vintage Books.

- Fowler, A. (1987). *History of English literature*. Cambridge, MA: Harvard University Press.
- Fox, S. (2000). *Trust and privacy online: Why Americans want to rewrite the rules*. Washington, DC: The Pew Internet and American Life Project.
- Fox, S., & Rainie, L. (2001). The online health care revolution: How the web helps Americans take better care of themselves. *American Journal of Health Systems Pharmacy*, 58, 107-108.
- Freud, S. (1911). *The interpretation of dreams* (A. A. Brill, Ed. and Trans.). New York: New York Press.
- Fried, C. (1968). Privacy. *The Yale Law Journal*, 77, 475-493.
- Gramm-Leach-Bliley Act, 15 U.S.C. § 6801-6809 (1999).
- Gray-Lukkarila, P. (1997). The right to privacy: Constitutional and theoretical foundations. *Dissertation Abstracts International*, 58 (05), 1892. (UMI No. 9730912)
- Griswold v. Connecticut, 381 U.S. 479 (1965).
- Harrison, C. L. (1993). The development of a desire for privacy scale. *Dissertation Abstracts International*, 54 (09), 4966. (UMI No. 9405263)
- Health and Human Services, Medicare Fraud hotline*. (2003). Retrieved February 15, 2003, from <http://www.hhs.gov/news/press/1997pres/970716.html>
- Health Insurance Portability Accountability Act, Pub. L. No. 104-191, 42 U.S.C. § 201 (1996).
- Hendersen, H. (1999). *Privacy in the information age*. New York: Facts on File.
- Hilden, J. (2002, October). CHIPPED: What legal questions are the new chip implants for humans likely to raise? *Cyberlaw*. Retrieved June 14, 2005, from http://practice.findlaw.com/archives/cyberlaw_1002.html
- HIPAA. (2001). Retrieved September 19, 2007, from <http://aspe.hhs.gov/admsimp/bannerps.htm>
- HIPAA Advisory Board. (2001, January-May). *Notes of meetings from the HIPAA advisory board*. Phoenix, AZ: Phoenix Health System.

Hippocrates, the Greek miracle in medicine, ancient medicine Medicina Antiqua. (400 BC). Francis Adams (Trans). Retrieved March 5, 2003, from <http://www.classics.mit.edu/Hippocrates/hipo oath.html>

Hobbes, T. (1651). *Leviathan: Or the matter, forme and power of a commonwealth ecclesiasticall and civil* (M. Oakeshoot, Ed.). New York: Macmillan.

Hofmann, M. A. (2001, April). Problems with privacy. *Business Insurance* 35, 6, 19.

Horne, D. R., & Horne, D. A. (1997). Privacy: A paranoid view. In M. Brucks & D. MacInnis (Eds.), *Advances in consumer research* (pp. 351-354). Provo, UT: Association for Consumer Research.

International Council of Nurses. (1953). *Nurses code of ethics: The ICN code of ethics for nurses*. Retrieved October 24, 2004, from <http://www.icn.ch/ethics.htm>

Jarvis-Thomson, J. (1975). The right to privacy. *Philosophy and Public Affairs*, 4, 295-314.

Johnson, C. A. (1975). Privacy as personal control. In D. H. Carson (Ed.), *Man-environment interactions: Evaluation and application, Vol. 6* (pp. 83-100). Washington, DC: Environment Design and Research Association.

Jorling, J., & Roach, W. (2002, February). Health information privacy: The preemption standard. *Topics in Health Information Management*, 5-16.

Katz v. United States, 389 U.S. 347 (1967).

Kennedy-Kassebaum Bill, 42 U.S.C. § 1397ii (1996).

Kouzoukas, D. (2002). HIPAA's privacy rule on research: Insight into the tension between privacy and the value of knowledge. *Boston HIPAA Forum*, 22, 13-20.

Lemov, P. (2002, March). The HIPAA headache. *Governing*, 15, 46-50.

Lind, M. (2002, January/February). Solving the privacy puzzle. *New Leader*, 15-17.

Locke, J. (1680-1690). *Two treatises on government*. Retrieved August 12, 2004, from <http://www.lonang.com/exlibris/locke>

Louis Harris and Associates. (1993). *Health care information privacy: A survey of the public and leaders* (Study No. 934009). New York: Louis Harris and Associates for Equifax.

Marriott International, Inc. (2001). [Marriott hotel directory]. Washington, DC: Author.

- McClellan, G. S. (Ed.). (1964). *Civil rights*. New York: The H. W. Wilson Press.
- McKesson Corporation. (2000, August). *Privacy in healthcare with the information age*. Paper presented at the meeting of Insight, Atlanta, GA.
- Meeler, D. W. (2000). Shared access and private space: A legal and philosophical analysis of privacy. *Dissertation Abstracts International*, 62 (01), 201. (UMI No. 3001468)
- Merriam-Webster Online*. (2004). Retrieved October 19, 2004, from <http://www.m-w.com/home/htm>
- Meyer v. Nebraska, 262 U.S. 390 (1923).
- Mill, J. S. (1859). *On liberty*. Indianapolis, IN: Bobbs-Merrill.
- Miller, A. (1971). *The assault on privacy*. Ann Arbor, MI: University Press.
- Milne, G. R., & Boza, M. E. (1999, Winter). Trust and concern in consumers' perceptions of marketing information management practices. *Journal of Interactive Marketing*, 5-24.
- Murphy, G. T. (1995). *Legislative information of the Internet, The Bill of Rights*. Retrieved October 25, 2004, from http://thomas.loc.gov/home/abt_thom.html
- N. A. A. C. P. v. Alabama, 357 U.S. 449 (1958).
- National Research Council. (1997). *For the record: Protecting electronic health information*. Washington, DC: National Academy Press.
- Nessen, C. (2001, Spring). Threats to privacy. *Social Research*, 68, 105-113.
- Nock, S. (1993). *The cost of privacy surveillance and reputation in America*. New York: Aldine De Gruyter.
- Norberg, P. A. (2003). Managed profiles: The value of personal information in commercial exchange. *Dissertation Abstracts International*, 64 (12), 4547. (UMI No. 3115636)
- Occupational Health and Safety Act of 1970, 29 U.S.C. § 657 (1970).
- Oliver, M. (1997). *History of philosophy*. New York: Barnes and Noble.
- Olmstead v. United States, 277 U.S. 438 (1928).

- Organization for Economic Development. (1991). *OECD statistics profile*. Retrieved May 3, 2007, from <http://www.oecd.org/us.html>.
- Patient Self Determination Act of 1990, 42 U.S.C. § 1395cc (1990).
- Paul, P. (2001, July). American demographics. *Mixed Signals*, 44-49.
- Pavesich v. New England Life Ins. Co., 50 S.E. 68 (Ga. 1905).
- Pierce v. Society of Sisters, 268 U.S. 510 (1925).
- Plato. (1968). *The republic of Plato* (A. Bloom, Trans.). New York: Basic Books.
- Popper, K. (1962). *The open society and its enemies*. Princeton, NJ: Princeton University Press.
- Posner, R. A. (1978). The economics of privacy. *Journal of Law and Society*, 71, 405-409.
- Poulsen, K. (2000). *Hospital records hacked* Retrieved June 21, 2004, from <http://www.securityfocus.com>
- Pozgar, G. (1996). *Legal aspects of healthcare administration* (6th ed.). Gaithersburg, MD: Aspen.
- Privacy Act, 5 U.S.C. § 552a (1974).
- Privacy concerns. (1999, February 11). *Ann Arbor News*, p. 4.
- Privacy Rule, Proposed Amendments to the HIPAA Privacy Rule § 164.506 Volume 22, 2002.
- Prosser, R. (1960). Privacy. *California Law Review*, 48, 383-423.
- Roberson v. Rochester Folding Box Company, 538: 64 N.E. 442 (N.Y. 1902).
- Roberts, L. A. (1993). *Ontology of privacy*. Unpublished doctoral dissertation, University of Oregon, Eugene.
- Roe v. Wade, 410 U.S. 113 (1973).
- Rosen, J. (2000). *The unwanted gaze*. New York: Random House.
- Ross, T. (1999, September). *Health service quality improvement and risk management*. Lecture conducted at Indiana University, South Bend, IN.
- Rotenburg, M. (2000). *The privacy law source book 2000*. Washington, DC: EPIC.

- Rousseau, J. J. (1762). *The social contract, principles of political right* (G. D. H. Cole, Trans.). Retrieved June 14, 2005, from <http://www.constitution.org> (Original work published 1762)
- Sargent, R. S. (2003, April). *Compelling state interest test*. Retrieved June 14, 2005, from <http://www.enterstageright.com>
- Schoeman, F. (1984). *The philosophical dimensions of privacy: The anthology*. Cambridge, MA: Cambridge University Press.
- Schwartz, P., & Leyden, P. (1997, July). The long boom: The history of the future 1980-2020. *Wired*, 15, 1-16.
- Self Determination Act*. (1990). Retrieved October 15, 2004, from <http://www.medical.upenn.edu/bioethic/museum>
- Senat, E. J. (2000). Privacy versus public access: An analysis of how courts balance these two competing social interests when government records are computerized. *Dissertation Abstracts International*, 61 (11), 4213. (UMI No. 9993378)
- Slutsman, J. (2004). Assessing physicians' attitudes toward the federal Health Information Privacy Rule (HIPAA Privacy Rule) and associated organizational compliance efforts. *Dissertation Abstracts International*, 64 (10), 4848. (UMI No. 3108175)
- Smith, A. (1776). *An inquiry into the nature and causes of the wealth of a nation*. London: T. Nelson and Sons.
- Smith, J. H. (1994). *Managing privacy information technology and corporate America*. Chapel Hill: University of North Carolina Press.
- Texas Penal Code of 1857, c. 7, Arts. 531-536; G. Paschal, Laws of Texas, Arts. 2192-2197 (1866); Texas Rev. Stat., c. 8, Arts. 536-541 (1879); Texas Rev. Crim. Stat., Arts. 1071-1076 (1911).
- Thompson, M. (1994). *Ethics*. Chicago: NTC.
- Time, Inc. v. Hill, 385 U.S. 374, 388 (1967).
- Tufts Managed Care Institute. (1998). *The healthcare system in the United States: Integrating cost and quality*. U. S. Health System, 1-3. Retrieved October 15, 2004, from <http://www.tnci.org/downloads/USHealthSystem.pdf>
- Unger, R. (1983). Unger's critique and synthesis. *American Journal of Jurisprudence*, 28, 118-148.

- University of Pennsylvania Bioethics. (1991). *Patient self determination rights* [Brochure]. Philadelphia, PA: Author.
- U.S. CONST. amend. IV.
- U.S. CONST. amend. XIV.
- Warden v. Hayden, 387 U.S. 294 (1967).
- Warren, S., & Brandeis, L. (1890). The right to privacy. *Harvard Law Review*, 4(5), 1-53.
- Wasserstrom, R. (1984). *Privacy: Some arguments and assumptions in philosophical dimensions of privacy* (F. D. Schoeman, Ed.). (Rev. ed.). Cambridge, MA: Cambridge University Press.
- Westin, A. F. (1967). *Privacy and freedom—Atheneum*. New York: The Association of the Bar of the City of New York.
- Wetterling Act of 1994, 42 U.S.C. § 14071 (1999).
- Whalen v. Roe, 429 U.S. 589 (1977).
- Whitaker, R. (1999). *The end of privacy: How total surveillance is becoming a reality*. New York: The New Press.
- Wiant, T. L. (2003). *Policy and its impact on medical record security*. Unpublished doctoral dissertation, University of Kentucky, Lexington.
- Wiretap Act of 1968, 18 U.S.C. §§ 2510-2522 (1968).
- Withrow, S. (2007). HIPAA compliance: Where are the savings? Retrieved July 5, 2007, from <http://www.wmolaw.com/hipaasavings.htm#where>.
- Wikipedia. (2006). *Due process*. Retrieved March 8, 2006, from http://en.wikipedia.org/wiki/Due_Process_Clause
- Wikipedia. (2007). *Humanities transparency*, Retrieved September 9, 2007, from [http://en.wikipedia.org/wiki/Transparency_\(humanities\)](http://en.wikipedia.org/wiki/Transparency_(humanities))
- Yuval, T. (1997). *Privacy and social norms: Social control by reputational costs*. Unpublished doctoral dissertation, University of Chicago Law, Chicago, IL.

VITA

VITA

Deborah Lange-Kuitse, RN, BSN, MHA
18280 Buckridge Ct. Goshen Indiana 46528

Career History

1998 to Present

McKesson Corporation, Healthcare Resource Management Group

Vice President of Research and Development for Anesthesia Management

Responsibilities include strategic planning and development for clinical applications including surgical and anesthesia research and development, re-engineering, market development, education, and ROI analysis)

1992-1998

Goshen General Hospital, Goshen Indiana

O.R. Information System Co-ordinator OR Management

Responsibilities include overall implementation, management and maintenance of the O.R and Cath Lab. Maintained all of Surgical Services case prepping, case history statistical analysis, supply/equipment and inventory/cost control. Maintained competencies programs for OR, Cath Lab, Day surgery, PACU and Pre-admission testing. Provided decision support and analysis to all of surgical services and medical staff.

Publications and Professional Associations

Publications: Nursing Economics, The Journal of AORN and Healthcare Informatics.

Member: AORN, Indiana State Nurses Association, Medical Ethics Council

Education

1999 - 2006, Andrews University

PhD candidate (Education Leadership)

1996 - 1998, Indiana University

MS in Health Administration and Public Affairs

1986 - 1989, Indiana University

BS in Nursing