

Regis University

ePublications at Regis University

Regis University Student Publications
(comprehensive collection)

Regis University Student Publications

Spring 2011

Mandated Government Regulations in Healthcare: Is Healthcare It Overregulated? a Post Mandate Study

Mark Albright
Regis University

Follow this and additional works at: <https://epublications.regis.edu/theses>



Part of the [Computer Sciences Commons](#)

Recommended Citation

Albright, Mark, "Mandated Government Regulations in Healthcare: Is Healthcare It Overregulated? a Post Mandate Study" (2011). *Regis University Student Publications (comprehensive collection)*. 430.
<https://epublications.regis.edu/theses/430>

This Thesis - Open Access is brought to you for free and open access by the Regis University Student Publications at ePublications at Regis University. It has been accepted for inclusion in Regis University Student Publications (comprehensive collection) by an authorized administrator of ePublications at Regis University. For more information, please contact epublications@regis.edu.

Regis University
College for Professional Studies Graduate Programs
Final Project/Thesis

Disclaimer

Use of the materials available in the Regis University Thesis Collection ("Collection") is limited and restricted to those users who agree to comply with the following terms of use. Regis University reserves the right to deny access to the Collection to any person who violates these terms of use or who seeks to or does alter, avoid or supersede the functional conditions, restrictions and limitations of the Collection.

The site may be used only for lawful purposes. The user is solely responsible for knowing and adhering to any and all applicable laws, rules, and regulations relating or pertaining to use of the Collection.

All content in this Collection is owned by and subject to the exclusive control of Regis University and the authors of the materials. It is available only for research purposes and may not be used in violation of copyright laws or for unlawful purposes. The materials may not be downloaded in whole or in part without permission of the copyright holder or as otherwise authorized in the "fair use" standards of the U.S. copyright laws and regulations.

**MANDATED GOVERNMENT REGULATIONS IN HEALTHCARE: IS HEALTHCARE
IT OVERREGULATED? A POST MANDATE STUDY**

A THESIS

SUBMITTED ON 30th DAY OF MARCH, 2011

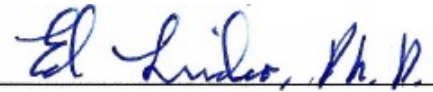
TO THE DEPARTMENT OF INFORMATION TECHNOLOGY
OF THE SCHOOL OF COMPUTER & INFORMATION SCIENCES
OF REGIS UNIVERSITY

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS OF MASTER OF SCIENCE IN
SYSTEMS ENGINEERING BY



Mark Albright

APPROVALS



Ed Lindoo, Thesis Advisor



Shari Plantz-Masters



Nancy Birkenheuer

Abstract

Over the past decade, healthcare organizations have been subjected to many federally mandated statutes to comply with. Three of the biggest statutes over the last decade are the Health Information Portability and Accountability Act (HIPAA), the Red Flag Rules, and the Health Information Technology for Clinical Health (HITECH). These mandates deal directly with the security of electronic patient information. To date, many entities have provided estimations of cost of compliance. Some have provided quantitative models to calculate the return of IT investments. Very few have attempted to look retrospectively and determine the level of and barriers to compliance. This quantitative study used a similar study as the framework to build upon. The study in part used survey questions from Mhamed Zineddine's doctoral dissertation titled, "Compliance of the healthcare industry with the Health Insurance Portability and Accountability Act security regulations in the Washington State: A quantitative study two years after mandatory compliance." The survey asked hospital Information Technology directors and managers questions to look at the level of compliance with the Health Insurance Portability and Accountability Act standards. Additionally, the survey asked questions to determine the impact on a health care organization when attempting to comply with multiple government mandates simultaneously. The analysis is an attempt to answer the question "Is Healthcare IT over regulated."

Acknowledgements

I acknowledge Mhamed Zineddine, Ph.D. for allowing me to use his research questions in this study. His generosity is very remarkable, thank you. Additionally, I acknowledge Mary Siegrist for her brilliance in statistics and her assistance with the data analysis. This study would not have been possible without her unselfish gift of assistance and direction. I cannot thank you enough.

I further acknowledge Karen Grossaint for her impressive editing skills and the words of encouragement she passed along to me. I appreciate and thank you for all of the help you provided me. Finally, I want to acknowledge my wife Kim. She was a tower of support, always providing me words of encouragement and praise. She always knew I would complete the work even when I had my own doubts. Thank you and I love you.

I dedicate this study and paper to my parents. Even though they have been gone for several years, I know they are proud of my accomplishment.

Table of Contents

| | |
|--------------------------------|----|
| 1. Introduction | 1 |
| Problem Statement | 5 |
| Research Questions | 6 |
| Study Significance | 7 |
| 2. Literature Review | 8 |
| 3. Methodology | 11 |
| Place | 11 |
| Participants | 12 |
| Instruments and Materials | 13 |
| Procedure | 16 |
| Data Analysis | 21 |
| 4. Results | 29 |
| Data Presentation and Analysis | 29 |
| 5. Discussion | 61 |
| Conclusions | 61 |
| Study Limitations | 65 |
| References | 68 |
| Appendix A | 71 |
| Appendix B | 80 |
| Appendix C | 82 |

List of Figures

| | | |
|----------|--|----|
| Figure 1 | Number of Years Employed With the Hospital | 31 |
|----------|--|----|

List of Tables

| | | |
|----------|--|----|
| Table 1 | Online Survey Responses | 21 |
| Table 2 | Frequencies on Demographic Data | 23 |
| Table 3 | Descriptive Statistics, Questions Measured by Scale | 24 |
| Table 4 | ANOVA Statistics | 26 |
| Table 5 | Measures of Association | 28 |
| Table 6 | Hospital Type | 30 |
| Table 7 | Total Number of Hospital Beds | 30 |
| Table 8 | Total Number of IT Employees | 31 |
| Table 9 | Highest Level of Education Obtained | 33 |
| Table 10 | Knowledge of HIPAA Security Rules | 34 |
| Table 11 | Knowledge of HITECH Security Standards | 35 |
| Table 12 | Knowledge of Red Flag Rules | 36 |
| Table 13 | HIPAA Budget Allocation by Year | 36 |
| Table 14 | Frequency of Security Risk Assessment | 38 |
| Table 15 | Implementation of HIPAA Security Measures | 38 |
| Table 16 | Implementation of HITECH Security Measures | 40 |
| Table 17 | Audit Logs, Access Reports, and Tracking Reports | 40 |
| Table 18 | Identification of a Security Official | 41 |
| Table 19 | Implementation of Workforce Access Procedures | 42 |
| Table 20 | Procedures for Terminating Access to PHI | 43 |
| Table 21 | User Authorization and Access Level to PHI | 44 |
| Table 22 | Guard Against, Detect, and Report Malicious Software | 45 |

List of Tables (Continued)

| | | |
|----------|--|----|
| Table 23 | Procedures to Create, Change, and Safeguard Passwords | 46 |
| Table 24 | Response and Reporting Procedures of Security Violations | 46 |
| Table 25 | Data Backup Plan | 47 |
| Table 26 | Disaster Recovery | 48 |
| Table 27 | Testing and Revising Contingency Plans | 49 |
| Table 28 | Assessing Specific Applications and Data | 50 |
| Table 29 | Business Associate Agreements in Place | 51 |
| Table 30 | Business Associate Agreements to Comply With HITECH | 52 |
| Table 31 | Safeguard Systems | 53 |
| Table 32 | Physical Safeguards for Workstations Accessing PHI | 54 |
| Table 33 | Encrypt and Decrypt | 55 |
| Table 34 | Security for Electronically Transmitted Information | 56 |
| Table 35 | Accounting of Disclosures | 56 |
| Table 36 | Security Standard Challenges Ranked by Mean | 57 |
| Table 37 | Fully Compliant With HIPAA, HITECH, and Red Flag | 59 |
| Table 38 | Difficulty Complying With Multiple Government Mandates | 60 |
| Table 39 | Compliance with Risk Analysis Requirement | 60 |

Chapter 1 – Introduction

In 1996, Congress enacted the Health Insurance Portability and Accountability Act, which is usually referenced as HIPAA (45 CFR Parts 160 and 164, I. Background, A. Statutory Background). The overall intent of Health Insurance Portability and Accountability Act was to improve the portability of health insurance and improve health insurance coverage by amending parts the Internal Revenue Code of 1986 (Public Law 104-191) . Also contained in the act was subtitle F, titled Administrative Simplification to make the health care system efficient and effective (Public Law 104-191) . The outcome of this goal was the implementation of a national health information system with prescribed standards and requirements.

When the law was enacted, it meant hospitals had to comply with the Administrative Simplification standards for electronic health information transactions, standards to protect a patient's health information, and the security of electronic health information systems. Each of the three set of standards included a compliance deadline; October 16, 2003 for electronic transactions, April 14, 2004 for health information privacy, and April 20, 2005 for the security standards. Compliance enforcement of the privacy and security standards fell under the authority of the Office for Civil Rights. The Office for Civil Rights could impose large civil money penalties for any noncompliance (45 CFR parts 160, 162, and 164 Health Insurance Reform: Security Standards, Summary) however; the Office fro Civil Rights lacked the necessary foot soldiers to enforce compliance.

Meeting the stated goals of the Health Insurance Portability and Accountability Act meant the adoption of new technologies that could improve the claims submission and paying process, provide instant information on insurance benefits and eligibility, and enhance other administrative processes. The adoption of an electronic medical record (EMR) and computerized

physician order entry systems (CPOE) meant instant access to health information for clinical decision making and safer delivery of the health care provided to patients. The Health Insurance Portability and Accountability Act provided a necessary framework to ensure health information and patient confidentiality protection. This security foundation would be critical to consider the development of a National Health Information Infrastructure (NHII).

Prior to April 20, 2005, the security standards implementation deadline, concerns were growing about the ability of hospitals to comply with the standards. In January 2005, the American Health Information Management Association conducted a survey to determine the state of hospital readiness with the security standards. With less than 4 months to comply with the standards, 26 percent of the survey respondents reported they were only 50% compliant and 12% reported they were less than 59% compliant (AHIMA, 2005).

As concerns regarding the nation's hospitals' level of compliance with the Health Insurance Portability and Accountability Act security standards grew, Having and Davis (2005) conducted a study to determine the progress made towards compliance. With less than three months to comply, Having and Davis reported that 32% of the respondents were less than 50 percent compliant with the security standards as written.

In May of 2008, Mhamed Zineddine, PhD, wrote a dissertation to satisfy the requirements for a Doctor of Philosophy degree. Zineddine conducted a quantitative study to determine how compliant hospitals in the state of Washington were with the Health Insurance Portability and Accountability Act security standards and any factors that may have been a barrier to compliance two years after the deadline for compliance (Zineddine, 2008). Zineddine concluded; hospitals in the state of Washington were 44.4 percent to 83.3 percent compliant depending on the number of Information Technology department employees employed at the

hospital (Zineddine, 2008). Zineddine's study cited four main contributing factors as barriers to compliance. Those factors ranked in order of significance were cost, implementation complexities, employee skill set, and understanding of the standards.

During the timeline for implementation of the Health Insurance Portability and Accountability Act security standards, hospitals were able to focus on that single government mandate in that it was the only government mandate at that time. Since the April 20, 2005 implementation deadline, several other Congressional Acts have been passed with mandated implementation dates including the Red Flag Rules and the Health Information Technology for Economic and Clinical Health Act security provisions, usually referred to as the HITECH security provisions and Meaningful Use requirements (<http://www.ahima.org/advocacy/arralegislationregulation.aspx>).

The Fair and Accurate Credit Transactions Act (FACT) became law in 2003. A sub component of FACT mandated the "detection, prevention, and mitigation of identity theft" (12 CFR parts 41, 222, 334 and 364, 571, 717, and 681 Identify Theft Red Flags). To that end, the Federal Trade Commission, the National Credit Union Administration and others co-authored the Red Flags Rule. The rules state that any business that has an "ongoing relationship with a person who is obtaining a product or service, albeit for personal, family, or household purposes, if that business allows deferment of payment", the business is a covered account and therefore; obligated to comply (Thornton, 2009). Healthcare organizations are covered accounts due to the deferred payment definition and, as such, must comply with the act.

A large component of Red Flag Rules compliance is policy and procedure development. A smaller component includes the use of technology to flag accounts that might have common data elements in them such as same social security numbers, same insurance identification

numbers, same driver's license numbers, and other person specific identifiers. Additionally, the rule required safeguards to protect unauthorized access to accounts with specific person identifiers. Failure to comply could be costly. Injured parties could file suit to seek damages. Additionally, the state attorney general could file class action suits under the unfair and deceptive acts and practices bill. Lastly, the federal courts could impose a fine up to \$16,000 per occurrence of theft (Thornton, 2009).

In 2009, the Secretary of the Department of Health and Human Services finalized the Health Information Technology for Economic and Clinical Health Act, a subcomponent of the American Recovery and Reinvestment Act commonly referred to as ARRA Public Law 111-5 or the "Stimulus Law." The fundamental tenet of the act seeks to increase and standardize the use of Electronic Health Records (EHR) in healthcare settings by making incentives, grants, and loans available to health care organizations who comply with the standards (Impac, 2010).

Hospitals that implement the meaningful use standards and demonstrate the use of those standards with a certified EHR as defined in the Health Information Technology for Economic and Clinical Health Act standards, could receive millions of dollars from the Centers for Medicare and Medicaid Services (CMS) based on an incentive payment calculation defined in the standards. Examples of the meaningful use requirements include the automation of processes, entering data into a certified system so that it resides in a structural format, and the implementation of ongoing routine security checks

(http://www.cms.gov/EHRIncentivePrograms/Downloads/Hosp_CAH_MU-TOC.pdf).

Recognizing shortcomings of the Health Insurance Portability and Accountability Act, the Health Information Technology for Economic and Clinical Health Act also attempts to strengthen the enforcement component of the original HIPAA standards by removing loopholes

and increasing penalties to a maximum of 1.5 million dollars. The Health Information Technology for Economic and Clinical Health Act incentivized law enforcement agencies to enforce compliance with the Health Insurance Portability and Accountability Act standards (45 CFR part 160 HIPAA Administrative Simplification: Enforcement, Summary). A key component of the improved enforcement standards is section 13411 of the standards, which requires the Secretary of the Department of Health and Human Services to ensure compliance with the Health Insurance Portability and Accountability Act security standards by conducting periodic audits of Covered Entities.

Problem Statement

These new mandates or subcomponents of the mandates impose implementation deadlines that are very close to each other. Complying with some of the standards of each of the mandates would be relatively simple since many of the standards are duplicative and overlapping. That said, there are many components that are specific to each of the mandates and require implementation of specific solutions. An additional barrier to full compliance is that the statutes assume a one size fits all approach, meaning regardless of size, budget, or geographical location, the organization must comply with the statutes as written. While the statutes are generally technology neutral, the cost of compliance could be a significant burden on a healthcare organization just as it was with the Health Insurance Portability and Accountability Act compliance. The Gartner Group estimated the cost of the Health Insurance Portability and Accountability Act compliance to be a staggering \$3.8 billion over a 5-year period between 2003 and 2005 (HIPAA Cost Considerations, 2003).

Since many hospitals were unable to comply fully with the mandated Health Insurance Portability and Accountability Act security standards, it is unlikely hospitals will be able to

achieve compliance when attempting to implement several government mandated standards simultaneously. Furthermore, hospitals that have not complied with the Health Insurance Portability and Accountability Act standards must circle back and achieve compliance before they can begin work on the new mandates. Similar to the Health Insurance Portability and Accountability Act, the standards for the new mandates are in Federal Registries and are difficult to understand. Implementation guidance is minimal and lacks the wisdom and the learned pitfalls of those with previous experience implementing the new standards (Zineddine 2008).

With the expressed permission of Mhamed Zineddine, PhD, this research project used the framework of Zineddine's study to build upon a minimal body of knowledge that currently exists in the health care industry. Specifically, the study looked at the level of compliance with the Red Flag Rules, the Health Information Technology for Economic and Clinical Health Act security provisions, and Meaningful Use requirements while hospitals continue to comply with the Health Insurance Portability and Accountability Act security standards. Additionally, this project looked at the significance implementing several government mandates simultaneously had on achieving compliance.

Research Questions

Absent of a significant body of knowledge that retrospectively examined the costs, benefits, and effectiveness of complying with federally mandated regulations in healthcare organizations, the thrust of this study was to determine if the Information Technology departments in healthcare organizations have been over regulated by analyzing the following questions:

1. What affect did federally mandated regulations have on achieving compliance?

2. What affect did complying with multiple mandates simultaneously over time have on the healthcare organization?
3. Did cost of implementation have any affect on the level of compliance?
4. If cost was a negative constraint in achieving compliance, were there other challenges and barriers to achieving compliance such as hospital size, geographical location, and perception or interpretation of the standards?
5. What impact did complying with government-mandated regulations have on the security of electronic patient information?
6. Do government mandated regulations achieve their intent?

Study Significance

Information regarding the compliance of government mandated regulations is virtually nonexistent or is proprietary and not intended for public review. This study was undertaken to build upon and to expand the breadth of research conducted by Mhamed Zineddine, PhD in 2008 that looked retrospectively at the level of HIPAA compliance that hospitals achieved in the state of Washington. The study provided a national perspective on the barriers to achieving compliance and in doing so, determined the power of a government mandate. Additionally, this study began to determine whether authors of federal statutes realize the desired outcomes of the intent of the regulations.

This study briefly explored overregulation of healthcare IT and the unanticipated negative effects on the industry. Since the body of knowledge regarding this subject matter is so limited, this study provides a basis for future researchers to expand research regarding overregulation and to provide their contributions, thereby growing this body of knowledge and perhaps impacting regulatory proposals as well as the overall process of compliance.

Chapter 2- Literature Review

Estimating the cost of complying with mandated government regulations prior to implementation is a common practice of the government. The General Office of Accounting provides estimations and embeds that information in the appropriate federal document. Many private organizations attempt to quantify the costs of regulatory compliance, usually in an attempt to justify the selling of their products or services. The SANS Institute provides information related to compliance activities to include costs. SANS suggested that the cost of the Health Insurance Portability and Accountability Act compliance would represent 100 percent to 150 percent of the efforts and costs related to the Y2K software modifications (SANS Institute, 2001). This information was found in one of their many educational offerings to provide guidance when complying with various federal regulations.

These reported costs are nothing more than estimates. These estimates could be useful if used as a best guess for budgetary purposes. The writer contends that these estimates are meaningless in that the data elements used to determine cost are at best a moving target. As an example, the cost of technology generally decreases over time. Additionally, the cost report does not take into consideration the various stages of compliance among hospitals and assumes a “ground zero” budget.

In 2005, Karen Having and Diane C. Davis did a follow-up survey of 286 hospitals from a random survey taken in 2004 to determine level of compliance towards the Health Insurance Portability and Accountability Act Security rule. The follow-up survey yielded a 50% return rate of the original respondents. Their results showed an overall improvement in the level of compliance; however, 32% of those respondents reported they were still less than 50% compliant with the standards as written, less than three months left to the deadline for implementation

(Having & Davis, 2005). While demonstrating the struggles to reach compliance, the study failed to identify the barriers to becoming compliant. This study was merely a spot check on the progress of compliance.

In addition to the many documents providing estimates on the cost of regulatory compliance, many sources recognize the shortage of information on the organizational value of their Information Technology investments secondary to regulatory compliance. Cavusoglu, Mishra, and Raghunathan recognized this shortcoming and provided a quantitative model to evaluate the return of security investment (ROSI) in an organization.

While useful, these estimates and models fall short in determining the organizational cost of complying with a federally mandated regulation. While attending Carnegie Mellon University, Arora and Pimental co-authored a thesis that attempted to determine the cost of complying with the Health Insurance Portability and Accountability Act for hospitals in the Pittsburgh area by “classifying and dissecting the most common expenses” associated with complying (Arora and Pimental, 2005). The study falls short of providing the total cost to comply with the Health Insurance Portability and Accountability Act regulation. Additionally, the study failed to recognize increased costs or decreased costs when complying with more than one mandated regulation over a period of prolonged time.

Mhamed Zineddine recognized that complying with the Health Insurance Portability and Accountability Act privacy standards, driven through the development of policies and procedures, was relatively easy to achieve compliance. However, the security rule required implementation of safeguards to prevent such incidents as intrusion. The implementation of the security technologies means compliance would be much more costly and likely have a negative impact on level of compliance achieved by each hospital. Zineddine’s quantitative research

demonstrated that several years after the deadline for compliance, it was nowhere near being achieved. He cited both the complexity of the rule and costs as being the two major barriers to compliance.

Zineddine's study also missed its mark for several reasons. The study was isolated to Washington State. He assumed he could extrapolate his findings to all "covered entities" mandated to comply with the Health Insurance Portability and Accountability Act. A significant flaw of the study was to include "covered entities" such as health plans and clearinghouses. These "covered entities" have both the financial and human resources to comply and likely would not encounter the same barriers to compliance as a hospital would. Additionally, they have different incentives to comply. Health plans and clearinghouses would be out of business if they failed to comply. Their existence depends and their ability to send, receive, and process electronic transactions and code sets as defined in the Health Insurance Portability and Accountability Act.

Another flaw this writer observed in the Zineddine study was his invited participants. He included CFO's, COO's, and others who likely did not have any first hand experience with the implementation. As such, the queried participants likely did not have the experience and the skill set to provide the response to his questions. Nonetheless, his research invites additional research and studies to determine the effectiveness of government mandated regulations and enforcement (Zineddine, 2008). The lack of an empirical body of knowledge in this area of research compels this writer to continue the research Zineddine presented in his 2008 dissertation at Capella University.

Chapter 3-Methodology

Mhamed Zineddine's 2008 study "Compliance of the healthcare industry with the Health Insurance Portability and Accountability Act security regulations in Washington State: a quantitative study two years after mandatory compliance" (Zineddine, 2008) provided the framework for this writer's study. Zineddine's quantitative study used a survey design methodology to quantify the level of hospital compliance with the Health Insurance Portability and Accountability Act in the state of Washington two years after the mandatory compliance date.

His study had a poor survey response rate of 3.77 percent (Zineddine, 2008). The writer attributed the poor survey response rate to the narrow geographical focus rather than survey design. Despite the poor survey response rate, the survey question provided responses necessary to answer the research questions.

As previously stated Zineddine's research provided the framework for this study. The methodology used in each study was very similar, a qualitative design. The writer used most of Zineddine's survey questions. Despite the similarities, this study design has numerous distinct differences noted when appropriate throughout this chapter.

Place

The definition of healthcare is "services offered by medical and allied health professions or relating to healthcare: the healthcare industry" (<http://medical-dictionary.thefreedictionary.com/health+care>). This broad definition could include clinics, physician offices, acute-care hospitals, rehabilitation hospitals, psychiatric hospitals, and other settings of healthcare services. To answer the research questions proposed in this paper, the scope of this study was limited to hospitals. Specifically, the study targeted acute-care hospitals

from each of the fifty states in the United States of America as a representation of the healthcare industry.

This study excluded teaching hospitals and hospitals that are part of a hospital network or system. Teaching hospitals have affiliations with learning institutions such as colleges and universities. These institutional affiliations could provide teaching hospitals an advantage over non-teaching hospitals in their ability to access human resources and funding. The inclusion of teaching hospitals would have introduced bias into the study.

Hospital networks or systems take advantage of the economies of scale through the centralization of their information technologies and resources and distribute them using various networking technologies and topologies. The inclusion of hospitals within a hospital network or system would potentially result in duplicative information or no information. To avoid the bias duplicative information would introduce and to keep the survey response rates high, this study excluded hospitals in a network or system.

Participants

This study targeted directors and managers of information technology departments of the targeted hospitals. Unlike the Zineddine study, this study excluded Chief Executive Officers, Chief Information Officers, Chief Financial Officers, and Chief Operations Officers. These positions seemed less likely to have the time to respond to a survey.

Attempts to find the names of the Information Technology department directors and managers were unsuccessful. As such, all survey invitations used a generic address to the manager or director of the information technology department. Each participant received a consent letter guarantying confidentiality and anonymity of each study participant.

Instruments and Materials

The limited body of knowledge regarding the level of compliance with government-mandated regulations in the healthcare industry drove the decision to use the framework of the Zineddine study to further that limited research. More specifically, Mhamad Zineddine, PhD gave written permission to use the survey questions form his 2008 dissertation.

Zineddine's survey consisted of 52 questions categorized into three distinct sections designed specifically to identify barriers to the implementation of the Health Insurance Portability and Accountability Act security rules and to determine the level of compliance with those rules. The first section consisted of demographic type questions and questions specific to hospital human resources. The second section asked specific questions centered on the administrative, physical, and technical components of the security rule. The third and last section consisted of the use of a Likert scale to rate factors Zineddine believed to be barriers to achieving compliance.

Despite the survey having been well designed, this writer identified several concerns with Zineddine's survey instrument. The questions targeted only the Health Insurance Portability and Accountability Act. His research went beyond hospitals and included physicians, healthcare clearinghouses, and health plans. Additionally, the targeted participants went beyond the Information Technology Director and Manager and included corporate attorneys, medical record directors, and chief information officers.

To use Zineddine's survey instrument, several modifications were required. When appropriate, the writer modified questions to include the Health Information Technology for Economic and Clinical Health Act security rules and Red Flag Rules (Appendix A). Two new questions were included about the level of compliance with the new security risk analysis

requirement and the pursuit of the meaningful use incentives. The final question count totaled 38 survey questions and one question included to accept or decline the informed consent provided to all potential participants. This writer preserved the survey's three-section format with the first section containing the demographic and human resource questions. The second section included questions aimed at the Health Insurance Portability and Accountability Act, the Health Information Technology for Economic and Clinical Health Act security rules, and Red Flag Rules. The third section contained an expanded version of the Likert scale to rate barriers to achieving compliance.

Thirty-three of the survey questions asked are questions based on level of measurement. These questions use an interval level of measurement. Several use a 1-5 bipolar scale, but the majority use a form of the Likert rating scale. Two of the interval questions fell into the cumulative category. Three of the 38 questions are dichotomous, using questions that have a yes or no answer or a variation of a yes or no answer. Two of the demographic questions asked allowed a fill in the blank response.

Questions edited from the Zineddine survey or added as new avoid loaded and leading language to prevent introducing response bias into the survey instrument. Mutually exclusive and exhaustive responses accompanied all closed-end questions avoiding accidental survey response bias. Similarly, this writer avoided double-barreled questions to prevent inaccuracies in the study measurements. The survey avoided ambiguity using clear and concise language in each question asked.

Validity and reliability are two terms that connote measurement of accuracy and credibility of the study's measurement instrument (Creswell, 2009). In other words, accuracy and credibility are predictors of error in the measurements. Specifically, validity indicates instrument

bias and reliability indicates error in the use of the instrument. Therefore, the accuracy and credibility of the measurement instrument directly influences the writer's ability to learn and draw conclusions from the data collected (Leedy & Ormrod, 2005).

The validity of the measurement instrument confirms that the instrument measures as designed. A valid study uses data to drive conclusions and enables the researcher to make extrapolations beyond the confines of the study (Leedy & Ormrod, 2005). Internal validity examines the relationships of data within the study, making it possible to examine all the explanations of the results increasing the confidence of the conclusions. External validity ensures the results are transferable or extrapolated to different contexts and populations outside of the study.

To achieve validity, the measuring instrument must be reliable. A reliable measurement instrument is one that provides consistent results (Leedy & Ormrod, 2005). Measurements of reliability are in actuality estimates. These general classifications of estimates include Inter-rater reliability, Test-retest reliability, Inter-method reliability, and Internal-consistency reliability. Single-administration and multiple-administration are the two most common methods of estimating reliability. The Pearson product-moment correlation coefficient is an example of multiple-administration estimation; an estimation of the same measure with two administrations (Shuttleworth, Martyn 2009). Internal-consistency is an example of a single-administration method. Cronbach's alpha is the most common Internal-consistency measurement (Choudhury, Amit 2010). Reliability of the research instrument improves through consistent administration of the instrument (Leedy & Ormrod, 2005).

Zineddine used both Face-validity and Content-validity methods to ensure the validity of his measuring instrument. Zineddine suggests that his use of an online tool to administer his

survey, inputting data directly into the database minimized random and unstable errors. He believed his measurement instrument demonstrated the necessary requirements to be valid and reliable. The writer extrapolates Zineddine's reasoning to conclude the current measuring instrument is valid and reliable.

Each study participant received a consent form (Appendix B). This two-page document provided the reader with an overview of the study, the procedure used to conduct the research for the study, the benefits and any risks of participation in the study, any alternative procedures that might be used, an explanation of what would be kept confidential and how it would be kept confidential. Additionally, the consent form contained instructions for anyone wishing to withdraw from the study and any related implications, the costs and compensation to the participant, and contact information of this writer, Regis University, and the advisor for the study. The consent form avoided confusion and ambiguity by using clear, concise language void of legal terms

Procedure

After an exhaustive literature search and subsequent review of that literature performed, this writer made the decision to use an existing quantitative study as a framework to contribute expanded research to a very limited body of knowledge. Mhamed Zineddine's research in his PhD dissertation; "Compliance Of The Healthcare Industry With The Health Insurance Portability And Accountability Act Security Regulations In Washington State: A Quantitative Study Two Years After Mandatory Compliance" attempted to answer research questions similar to the questions presented in this study (Zineddine, 2008). This writer opted to use Zineddine's well-designed survey questions with some minor edits and modifications to the survey instrument.

An Internet search found Mhamed Zineddine to be a business owner in the State of Washington. Despite being a business owner in the United States, he returned to Dubai, one of the seven emirates of the United Arab Emirates. Zineddine's business partner offered this writer his e-mail address. This writer used an e-mail to provide an explanation of this study and requested permission to use the survey questions from Zineddine's dissertation. Zineddine granted permission to use the survey questions in an e-mail response.

Upon receiving permission to use the survey questions, the writer completed the institutional review board (IRB) application to request an IRB exemption and approval to proceed with the study. The Regis University IRB gave permission to proceed with the study as submitted.

A 2009 report from the American Hospital Association puts the total number of registered hospitals in the United States at 5,708 (American Hospital Association, 2009). According to Gay, when $N=5,000$ or greater, the population size becomes irrelevant and the sample size around 400 is sufficient. Accordingly, the writer settled on a sample size of 300 hospitals (Gay, 2009). Questionnaire return rates average around 50% or lower (Leedy & Ormrod, 2005). To ensure an adequate sample size, the number of targeted hospitals was double the desired sample size or 600 hospitals. Use of a stratified random sampling design minimized the introduction of bias into the sampling process (Leedy & Ormrod, 2005).

The target for the study included hospitals from all 50 United States. To target specific hospitals, the number of beds provided a method to stratify the hospitals. Stratification categories used number of beds from 0-75, 76-150, 151-250, and 251-500, creating four distinct categories of hospitals. To determine the number of hospitals needed for each category per each state, the writer used the following formula: 600 hospitals divided by four categories divided by 50 United

States. To achieve the targeted number of surveys, the writer identified three hospitals from each of the four categories from every state.

Hospital identification used area codes from each state to achieve an equal blending population sample. Searching the Internet, the writer listed all of the area codes for all 50 states in alphabetical order. Using the American Hospital Directory website, the writer entered an area code from the first state in the alphabet into the search field of the website. The website pulled all of the hospitals from the area code in alphabetical order in a column. Each hospital displayed the city it resided in and the number of beds registered to the hospital. From the display of hospitals, the writer had access to the Uniform Resource Locator (URL) link if the hospital had a website.

To list a hospital on the target list, the writer looked for a hospital with a website from each of the four categories. The writer accessed the website to confirm the hospital was not a teaching facility or part of a hospital system or network. If a hospital fit the criteria, the writer listed the name, address, main phone number, Information Technology Department phone number if listed, name of Information Technology Department director or manager if listed, and the URL on a spreadsheet.

The writer used one hospital per each category per area code to ensure geographical equal blending. In states with a limited number of area codes, the writer used an area code multiple times if necessary. If a state did not have enough hospitals to fill one or more of the four categories, the writer reduced the number of hospitals from one category and increased another category by the same amount of the reduction. As an alternative, the writer made an additional selection from the needed category from a neighboring state.

Once the writer completed the hospital identification process, the writer contacted each hospital in an attempt to identify the Information Technology Department director or manager and his or her contact information. Any information provided completed the spreadsheet. The spreadsheet then became a tool for a mail merge and mailing labels.

Choosing the interview methodology proved a simple process. The use of web surveys gained dramatically on the use rate of telephone surveys. The latest estimates state that 96% of homes in the United States have a phone (Knowledge-base. super survey.com). The website Internet World Stats cites the 2010 North American population at 344,124,450 people of which 266,224,500 are Internet users or a 74% penetration rate. Despite having the slowest 10-year growth between 2000 and 2010 when compared to six other world regions, the United States posted an Internet use rate growth of 146.3% in the same period (Internetworldstats.com). Considering variables such as time, budget, and human resources, the writer ruled out the use of a phone survey.

The targeted participants are both highly literate and technology savvy. Because the targeted participants are highly literate, the writer considered the use of a mailed survey. Mailed surveys typically yield a 20% response rate (knowledge-base.supersurvey.com). The survey design targeted a 50% response rate thereby ruling out the use of a mailed survey. A web survey lends itself to covering a large geographical area in a relatively cheap and expeditious way. The reasons already stated dictated the use of a web survey. To that end, the writer set up an account with Zoomerang.com, an Internet survey software tool.

The writer built the survey instrument using the online software tool and published the survey to a test site. The writer deployed the test-site survey URL to five non-participants who tested the mechanics of taking the survey, time necessary to complete the survey, and analyzed

the survey for grammatical and spelling error. Once appropriately tested and all necessary edits completed, the writer copied the survey from the test site to the live environment.

Zineddine (2008) ensured his measurement instrument demonstrated validity and reliability. He achieved this status with a pilot survey; making the necessary edits based on the responses received. Using Zineddine's measurement instrument with minor modifications and deletions, the writer did not think testing for validity and reliability was necessary at this time. The instrument would be retested for validity and reliability once the study yielded results; creating a quasi-pilot survey.

A letter of introduction that accompanied the informed consent instrument contained a short introduction to the writer, a short description of the study, approximate time necessary to complete the survey, the survey site URL, and a profound thank you for the participation (Appendix C). After stuffing the introduction letter and surveys into addressed envelopes, the writer mailed all 600 envelopes on December 5, 2010. The timing of the dissemination of the survey to the participants competed directly with the Christmas holiday and New Year celebration. In an attempt to maximize the response rate, the writer extended the survey access through January 2011.

To compensate for the writer's limited knowledge and skill-set in statistical analysis and to ensure an accurate and valid analysis the writer queried the University of Northern Colorado's Applied Statistics and Research Methods Department for assistance with statistical analysis of this study. In response to the writer's query, a PhD student with a concentration in research methods agreed to assist with the analysis of findings.

Data Analysis

After the extension of the survey completion timeline expired, the writer extracted all results submitted via the online survey tool and entered them into the database. Consistency and integrity database checks provided confidence regarding the data submitted. As stated previously, the writer planned to test the validity and reliability of this measurement instrument and compare the results to those of Zineddine (2008). As noted in Table 1, the low response rate of 3.16% nullified the desire to test the validity and reliability of the measuring instrument.

Table 1

Online Survey Responses

| | Frequency | Percent | Valid Percent | Cumulative Percent |
|------------------|-----------|---------|------------------|-----------------------|
| Survey Responses | 19 | 3.16 | 3.16 | 3.16 |

The writer received two email questions from two of the study participants asking for clarification of the URL provided. In both cases, the participants transposed the letter O for a zero. Based on the type and number of questions asked, the writer made the assumption that the survey was concise and clearly written, lacking confusion and misunderstanding.

The study intended to answer the following six research questions:

1. What affect did federally mandated regulations have on achieving compliance?
2. What affect did complying with multiple mandates simultaneously over time have on the healthcare organization?
3. Did cost have any affect on the level of compliance?

4. If cost was a negative constraint in achieving compliance, were there other challenges and barriers to achieving compliance such as hospital size, geographical location, and perception or interpretation of the standards?
5. What impact did complying with government-mandated regulations have on the security of electronic patient information?
6. Do government-mandated regulations achieve their intent?

To answer these questions, the survey used Zineddine's (2008) questions designed using the Health Insurance Portability and Accountability Act federal regulations (Federal Register / Vol. 70, No. 198 /Friday, October 14, 2005) and then modified by the writer using the HITECH and Red Flag Rules federal regulations. The writer looked for the existence of causal relationships of the variables researched to achieve the task.

Using SPSS software, the writer's assistant compiled descriptive and frequency calculations to determine the features of the data and what the data indicates. The statistical calculations included distribution, central tendency, and dispersion. More specifically, as noted in Table 2, the demographic survey questions representing nominal, ordinal data used frequency calculations to determine distributions.

Table 2

Frequencies on Demographic Data

| | | Profit Status | Zip Code | No Beds | No Employee |
|---|------------------------|---------------|-------------|------------|-------------|
| | | Financial | Zip Code | Total # of | Total # IT |
| | | Status of | Zip Code of | Total # of | Total # IT |
| | | Hospital | Hospital | beds | employees |
| N | Valid | 19 | 19 | 19 | 19 |
| | Missing | 0 | 0 | 0 | 0 |
| | Skewness | 2.798 | -.352 | .437 | .389 |
| | Std. Error of Skewness | .524 | .524 | .524 | .524 |
| | Kurtosis | 6.509 | -1.178 | -.128 | -1.374 |
| Table 2 Frequencies on Demographic Data (Continued) | | | | | |
| | Std. Error of Kurtosis | 1.014 | 1.014 | 1.014 | 1.014 |

Table 2

Frequencies on Demographic Data Continued

| | | Yrs | Education | HIPAA |
|---|------------------------|----------|-----------|-----------|
| | | Employed | Highest | Knowledge |
| | | Years | Level of | HIPPA |
| | | Employed | Education | Knowledge |
| N | Valid | 19 | 19 | 19 |
| | Missing | 0 | 0 | 0 |
| | Skewness | .033 | .473 | -2.798 |
| | Std. Error of Skewness | .524 | .524 | .524 |
| | Kurtosis | -1.087 | .641 | 6.509 |
| | Std. Error of Kurtosis | 1.014 | 1.014 | 1.014 |

Shown in Table 3 are the survey questions measured by use of scale using descriptive statistical calculations to determine central tendency and dispersion.

Table 3

Descriptive Statistics on Questions Measured by Scale

| | N | Min | Max | Mean | Std. Deviation | Skewness |
|---------------------|-----------|-----------|-----------|-----------|-------------------|-----------|
| | Statistic | Statistic | Statistic | Statistic | Statistic | Statistic |
| HITECHKnow | 19 | 1 | 2 | 1.68 | .478 | -.862 |
| HITECH Knowledge | | | | | | |
| RedFlagKnow Red | 19 | 0 | 2 | 1.16 | .602 | -.047 |
| Flag Rule Knowledge | | | | | | |
| Q2010 2010 | 11 | 1 | 1 | 1.00 | .000 | . |
| Q2009 2009 | 8 | 1 | 1 | 1.00 | .000 | . |
| Q2008 2008 | 6 | 1 | 1 | 1.00 | .000 | . |
| Q2007 2007 | 6 | 1 | 1 | 1.00 | .000 | . |
| Q2006 2006 | 6 | 1 | 1 | 1.00 | .000 | . |
| Q2005 2005 | 4 | 1 | 1 | 1.00 | .000 | . |
| Q2004 2004 | 4 | 1 | 1 | 1.00 | .000 | . |
| Q2003 2003 | 4 | 1 | 1 | 1.00 | .000 | . |
| QBudget | 6 | 1 | 1 | 1.00 | .000 | . |
| Q1 | 1 | 1 | 1 | 1.00 | . | . |
| SecurityMeasures | 19 | 0 | 7 | 4.00 | 2.449 | -.152 |
| ImplementSecMeasure | 19 | 0 | 8 | 4.53 | 3.878 | -.332 |
| SystemsRevRecords | 19 | 0 | 10 | 5.79 | 3.896 | -.459 |
| IDSecurityOfficial | 19 | 0 | 10 | 7.42 | 3.115 | -1.327 |
| WorkforceAsses | 19 | 1 | 10 | 7.53 | 2.913 | -.829 |
| TermPHIAccess | 19 | 1 | 10 | 8.00 | 2.494 | -1.752 |
| UserAuth | 19 | 1 | 10 | 7.53 | 2.736 | -1.114 |
| GuardDetect | 19 | 1 | 9 | 7.26 | 2.579 | -1.173 |
| CreateChange | 19 | 1 | 10 | 8.26 | 2.077 | -2.719 |
| RRProcedures | 19 | 0 | 10 | 7.21 | 3.326 | -1.167 |
| Backup | 19 | 1 | 9 | 8.11 | 2.233 | -2.488 |
| RecoveryPlan | 19 | 0 | 9 | 5.26 | 4.254 | -.349 |
| PeriodicTesting | 19 | 0 | 10 | 4.16 | 4.100 | .317 |
| AssessSpecificApps | 19 | 0 | 10 | 6.16 | 3.219 | -.740 |
| BAA | 19 | 1 | 10 | 8.11 | 2.807 | -1.401 |

Table 3 Descriptive Statistics on Questions Measured by Scale (Continued)

| | | | | | | |
|----------------------|----|---|----|------|-------|--------|
| HITECHBAA | 18 | 0 | 1 | .83 | .383 | -1.956 |
| Safeguard | 19 | 1 | 10 | 7.42 | 2.673 | -.994 |
| WorkstationSafeguard | 19 | 0 | 10 | 7.05 | 3.308 | -.855 |
| Encrypt | 19 | 0 | 10 | 4.58 | 4.087 | -.070 |
| ElectronicTrans | 19 | 0 | 10 | 4.37 | 4.072 | .193 |
| BreachprocessPP | 19 | 0 | 1 | .79 | .419 | -1.545 |
| HIPPAChallenges | 0 | | | | | |
| Ambiguity | 18 | 2 | 5 | 3.06 | .802 | .663 |
| Misunderstanding | 18 | 1 | 5 | 3.11 | .900 | -.237 |
| Abscertprocess | 18 | 2 | 5 | 3.61 | .916 | -.110 |
| lackintcompliance | 18 | 2 | 5 | 3.83 | 1.043 | -.330 |
| cost | 18 | 1 | 4 | 2.56 | 1.042 | .010 |
| lackexpertisec | 18 | 2 | 5 | 3.50 | 1.150 | -.130 |
| abseffectiveldrshp | 18 | 1 | 5 | 3.83 | 1.150 | -1.202 |
| complexityrules | 18 | 1 | 4 | 2.61 | 1.092 | -.014 |
| lackexpHIPAAsec | 18 | 2 | 5 | 3.78 | 1.060 | -.503 |
| lackexpHITECHRedfla | 18 | 2 | 5 | 3.67 | .970 | -.097 |
| ComplyHITECHRedFl | 0 | | | | | |
| ChangePP | 18 | 1 | 1 | 1.00 | .000 | . |
| Addlstafftraining | 16 | 1 | 1 | 1.00 | .000 | . |
| RevSecurityPP | 17 | 1 | 1 | 1.00 | .000 | . |
| AddlInvestments | 13 | 1 | 1 | 1.00 | .000 | . |
| Compliantlevel | 19 | 0 | 2 | .79 | .976 | .468 |
| compliancedifficulty | 19 | 0 | 2 | 1.00 | .745 | .000 |
| riskassesscompliance | 19 | 0 | 2 | .84 | .602 | .047 |
| meaningfuluse | 19 | 1 | 1 | 1.00 | .000 | . |
| Valid N (listwise) | 0 | | | | | |

The use of inferential statistics provided the bases for making generalizations regarding the entire population from the sampled data. As noted in Table 4, the general linear model Analysis of Variance (ANOVA), provided the test to determine if equality existed between the means provided.

Table 4

ANOVA Statistics

| | | Sum of Squares | df |
|---------------------|--------------------|-------------------|----|
| RedFlagKnow Red | Between (Combined) | .219 | 1 |
| Flag Rule Knowledge | Groups | | |
| * HITECHKnow | Within Groups | 6.308 | 17 |
| HITECH Knowledge | Total | 6.526 | 18 |

a. With fewer than three groups, linearity measures for RedFlagKnow, Red Flag Rule Knowledge *, HITECHKnow or HITECH Knowledge cannot be computed.

Table 4 ANOVA Statistics (Continued)

| | | Mean Square | F | Sig. |
|-----------------------|--------------------|----------------|------|------|
| RedFlagKnow Red | Between (Combined) | .219 | .589 | .453 |
| Flag Rule Knowledge * | Groups | | | |
| HITECHKnow | Within Groups | .371 | | |
| HITECH Knowledge | Total | | | |

. With fewer than three groups, linearity measures for RedFlagKnow, Red Flag Rule Knowledge *, HITECHKnow or HITECH Knowledge cannot be computed.

Table 4 ANOVA Statistics (Continued)

| | | Sum of Squares | df | Mean Square |
|----------------------|---------------|-------------------|----|----------------|
| HITECHKnow | Between | .076 | 1 | .076 |
| HITECH Knowledge | Groups | | | |
| | Within Groups | 4.029 | 17 | .237 |
| | Total | 4.105 | 18 | |
| RedFlagKnow Red Flag | Between | .967 | 1 | .967 |
| Rule Knowledge | Groups | | | |
| | Within Groups | 5.559 | 17 | .327 |
| | Total | 6.526 | 18 | |

Table 4 ANOVA Statistics (Continued)

| | | | | |
|----------------------|----------------|---------|----|--------|
| SecurityMeasures | Between Groups | .559 | 1 | .559 |
| | Within Groups | 107.441 | 17 | 6.320 |
| | Total | 108.000 | 18 | |
| ImplementSecMeasures | Between Groups | .619 | 1 | .619 |
| | Within Groups | 270.118 | 17 | 15.889 |
| | Total | 270.737 | 18 | |
| SystemsRevRecords | Between Groups | 17.393 | 1 | 17.393 |
| | Within Groups | 255.765 | 17 | 15.045 |
| | Total | 273.158 | 18 | |
| IDSecurityOfficial | Between Groups | .749 | 1 | .749 |
| | Within Groups | 173.882 | 17 | 10.228 |
| | Total | 174.632 | 18 | |
| WorkforceAsses | Between Groups | 14.266 | 1 | 14.266 |
| | Within Groups | 138.471 | 17 | 8.145 |

Table 4 ANOVA Statistics (Continued)

| | | F | Sig. |
|--|----------------|-------|------|
| HITECHKnow HITECH Knowledge | Between Groups | .320 | .579 |
| | Within Groups | | |
| | Total | | |
| RedFlagKnow Red Flag Rule Knowledge | Between Groups | 2.959 | .104 |
| | Within Groups | | |
| | Total | | |
| SecurityMeasures | Between Groups | .088 | .770 |
| | Within Groups | | |

Table 4 ANOVA Statistics
(Continued)

| Within Groups | | | |
|---------------------|---------|------|------|
| Total | | | |
| ImplementSecMeasure | Between | .039 | .846 |
| Groups | | | |
| Within Groups | | | |

In statistics, an association is a term that connotes a broad relationship of two statistically dependent quantity measurements depicted in Table 5. The term “association” implies a causal relationship of the two statistically dependent quantities does not exist (Upton & Cook, 2006). The term “correlation” provides a narrower definition of relationship connoting a linear relationship with two quantities.

Table 5
Measures of Association

| | Eta | Eta Squared |
|---------------------|------|-------------|
| RedFlagKnow Red | .183 | .033 |
| Flag Rule Knowledge | | |
| * HITECHKnow | | |
| HITECH Knowledge | | |

A review of Table 5, Measurements of Association raise concerns regarding effect size. When discussing eta-squared, 0.2 is a small effect, 0.5 is a medium effect, and 0.8 is a large effect (Cohen, 1988). With an eta-squared of 0.033, the study is lacking statistical significance due to the extremely low survey response rate. The writer discusses the consequence of the lack of statistical significance in detail in the following chapter.

Chapter 4 – Results

Data Presentation and Analysis

In world of statistics, when the result likely occurred by chance, the result is not statistically significant. Conversely, the result is significant if the occurrence was not due to chance (<http://faculty.vassar.edu/lowry/ch4pt1.html>). For most researchers, the believable level is 95%. The measurement of believability is the inverse of believability or 0.05, meaning there is a five percent chance that the result is not true. The significance level or the evidence required for believability is the critical p-value (Stigler S 2008). The p-value has a direct relationship to results reliability. The greater the p-value, the greater the probability the result occurred by chance. Sample size influences the significance of the results. Large sample sizes will detect small differences in results and quantify the differences as significant.

Lacking statistical significance or believability, the writer is unable to use the data to answer the research questions with any certainty. Any answers rendered would merely be conjecture or an assumption. Instead, the writer will display data and compare the data from this study to the data obtained in Zineddine's (2008) study.

The first section discussed includes demographic information to include hospital type, bed size, geographical location, number of Information Technology employees, length of employment of the participants, and level of education. As Table 6 demonstrates, 89.47 of the participants are employed in a not for profit hospital. Conversely, only 62.5% of the participants in Zineddine's (2008) study were employed at a not for profit organization. Of the 50 United States, the study represents participants from 28% of the United States. The geographical regions represented include 26.32% from the Central Plains, 10.53% from the Northern Plains, 5.26% from the North Wets, 15.79% from the Central Rockies, 21.05% from the North East, 5.26%

from the South East, 10.53% from the Mid West, and 5.26% from Mid Atlantic area. Fifty-two percent of the responses came from states in the middle of the country.

Table 6

Hospital Type

| | Frequency | Percent | Valid Percent | Cumulative Percent |
|----------------|-----------|---------|---------------|-----------------------|
| Not for Profit | 17 | 89.47 | 89.47 | 89.47 |
| For Profit | 2 | 10.53 | 10.53 | 100 |
| Total | 19 | 100 | 100 | |

Table 7 shows that 52.64% of the participants work in a hospital with bed size ranging from 101 beds to 300 beds.

Table 7

Total Number of Hospital Beds

| | Frequency | Percent | Valid Percent | Cumulative Percent |
|---------|-----------|---------|---------------|-----------------------|
| 5-50 | 5 | 26.32 | 26.32 | 26.32 |
| 51-100 | 1 | 5.26 | 5.26 | 31.58 |
| 101-200 | 5 | 26.32 | 26.32 | 57.9 |
| 201-300 | 5 | 26.32 | 26.32 | 84.22 |
| 301-400 | 1 | 5.26 | 5.26 | 89.48 |

Table 7 Total Number of Hospital Beds (Continued)

| | | | | |
|---------|----|------|------|-------|
| 401-500 | 1 | 5.26 | 5.26 | 94.74 |
| >500 | 1 | 5.26 | 5.26 | 100 |
| Total | 19 | 100 | 100 | |

Of the hospitals represented in this study, 36.83% have between 1 and 10 Information Technology Department employees. Over 26% of the hospitals have greater than 51 employees (see Table 8). Zineddine (2008) included institutions other than hospitals such as health plans and healthcare clearinghouses. As such, the writer did not make comparisons to Zineddine's results in that both health plans and healthcare clearinghouses employ a greater number of employees than this study's scale for number of employees.

Table 8

Total Number of Employees in the Information Technology Department

| | Frequency | Percent | Valid Percent | Cumulative Percent |
|--------|-----------|---------|---------------|-----------------------|
| 1-10 | 7 | 36.83 | 36.83 | 36.83 |
| 11-20 | 2 | 10.53 | 10.53 | 47.36 |
| 21-50 | 5 | 26.32 | 26.32 | 73.68 |
| 51-100 | 3 | 15.79 | 15.79 | 89.47 |
| >100 | 2 | 10.53 | 10.53 | 100 |
| Total | 19 | 100 | 100 | |

Figure 1 shows a 9.18 mean length of participant employment with the hospital they represent. Zineddine (2008) asked the question differently; therefore, the writer did not compare this question to Zineddine's responses. The last question asked in this section asks the level of education of each of the participants. Table 9 shows 57.89% of the responding participants have a four year undergraduate college degree. Moreover, 89.47% of all the participants report a four year undergraduate college degree or greater.

Figure 1

Number of Years Employed With the Hospital

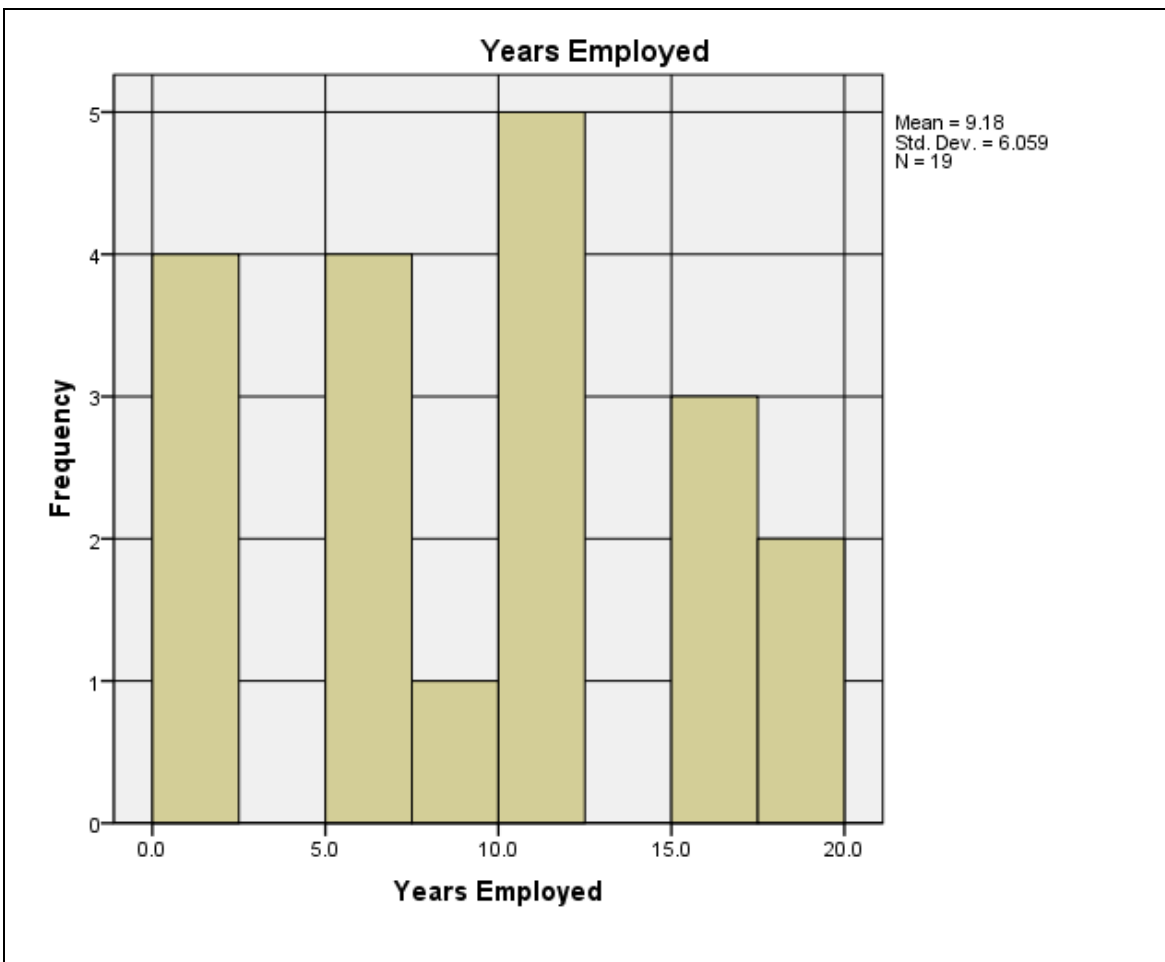


Table 9

Highest Level of Education Obtained

| | Frequency | Percent | Valid Percent | Cumulative Percent |
|------------------------------|-----------|---------|---------------|-----------------------|
| High-School/GED | 0 | 0 | 0 | 0 |
| Some College | 2 | 10.53 | 10.53 | 10.53 |
| 2-Year College Degree | 0 | 0 | 0 | 10.53 |
| 4-Year College Degree | 11 | 57.89 | 57.89 | 68.42 |
| Master's Degree | 5 | 26.32 | 26.32 | 94.74 |
| Doctoral Degree | 0 | 0 | 0 | 94.74 |
| Professional Degree (MD, JD) | 1 | 5.26 | 5.26 | 100 |
| Other | 0 | 0 | 0 | 100 |
| Total | 19 | 100 | 100 | |

The following section displays results and interpretations of questions aimed at the Health Insurance Portability and Accountability Act, the Health Information Technology for Economic and Clinical Health Act security rules, and Red Flag Rules. The results of these questions analyzed using measurements of scale. When appropriate, the writer compares the data with Zineddine's (2008) responses.

The first series of questions discusses the level of participant knowledge of each of the government-mandated regulations. Table 10 shows that 89.47% of the participants feel they are very knowledgeable about the Health Insurance Portability and Accountability Act security rules. In 2008, only 50% of Zinzeddine's (2008) respondents felt they were very knowledgeable about the Health Insurance Portability and Accountability Act security rules. The writer hypothesizes that when the government mandated the 2009 Health Information Technology for Economic and Clinical Health Act, participants were obligated to revisit the Health Insurance Portability and Accountability Act security rules to gain the necessary knowledge to comply with the Health Information Technology for Economic and Clinical Health Act.

Table 10

Knowledge of the HIPAA Security Rules

| | Frequency | Percent | Valid Percent | Cumulative Percent |
|---------------------------|-----------|---------|---------------|-----------------------|
| Very Knowledgeable | 17 | 89.47 | 89.47 | 89.47 |
| Somewhat Knowledgeable | 2 | 10.53 | 10.53 | 100 |
| Not Knowledgeable | 0 | 0 | 0 | 100 |
| Total | 19 | 100 | 100 | |

In comparison to the reported knowledge regarding the Health Insurance Portability and Accountability Act security rules, Table 11 shows that only 68.42% of the participants reported

being very knowledgeable about the Health Information Technology for Economic and Clinical Health Act security standards. Zineddine's (2008) study surveyed participants only about the Health Insurance Portability and Accountability Act; therefore, the writer could not make any comparisons between the studies.

Table 11

Knowledge of the HITECH Security Standards

| | Frequency | Percent | Valid Percent | Cumulative Percent |
|---------------------------|-----------|---------|---------------|-----------------------|
| Very Knowledgeable | 13 | 68.42 | 68.42 | 68.42 |
| Somewhat Knowledgeable | 6 | 31.58 | 31.58 | 100 |
| Not Knowledgeable | 0 | 0 | 0 | 100 |
| Total | 19 | 100 | 100 | |

Table 12 shows 26.32% of the participants feel they are very knowledgeable about the Red Flag Rules. The writer hypothesizes that hospitals were confused about whether the mandate applied to them, which slowed the process of learning about the mandate. A recent government clarification says that hospitals must comply with the mandate.

Table 12

Knowledge of the Red Flag Rules

| | Frequency | Percent | Valid Percent | Cumulative Percent |
|---------------|-----------|---------|---------------|-----------------------|
| Very | 5 | 26.32 | 26.32 | 26.32 |
| Somewhat | 12 | 63.15 | 63.15 | 89.47 |
| Knowledgeable | | | | |
| Not | 2 | 10.53 | 10.53 | 100 |
| Knowledgeable | | | | |
| Total | 100 | 100 | 100 | |

The following data and interpretations reflect responses to detailed questions regarding processes centered on the Health Insurance Portability and Accountability Act. Table 13 shows 31.58% of the participants said their respective hospitals have not budgeted for any of the Health Insurance Portability and Accountability Act components since 2003. One survey participant responded by saying he or she did not know if a budget had been allocated. Only 15.79% of the participants stated their respective hospitals had created a Health Insurance Portability and Accountability Act budget every year from 2003.

Table 13

HIPAA Budget Allocation by Year

| | Frequency | Percent | Valid Percent | Cumulative Percent |
|--|-----------|---------|---------------|-----------------------|
|--|-----------|---------|---------------|-----------------------|

| | | | | |
|------------------|----|-------|-------|-------|
| 2003, 2004, | 3 | 15.79 | 15.79 | 15.79 |
| 2005, 2006, | | | | |
| 2007, 2008, | | | | |
| 2009, 2010 | | | | |
| 2003, 2004, | 1 | 5.26 | 5.26 | 21.05 |
| 2005, 2006, | | | | |
| 2007, 2009, | | | | |
| 2010 | | | | |
| 2006, 2007, | 1 | 5.26 | 5.26 | 26.31 |
| 2008, 2009, 2010 | | | | |
| 2006, 2007, 2010 | 1 | 5.26 | 5.26 | 31.57 |
| 2008, 2009, 2010 | 1 | 5.26 | 5.26 | 36.83 |
| 2009, 2010 | 2 | 10.54 | 10.54 | 47.37 |
| 2010 | 3 | 15.79 | 15.79 | 63.16 |
| None | 6 | 31.58 | 31.58 | 94.74 |
| Don't know | 1 | 5.26 | 5.26 | 100 |
| Total | 19 | 100 | 100 | |

Table 13 shows cost could have played some role in complying with the Health Information Technology for Economic and Clinical Health Act security standards but does not identify what role it played or how it affected compliance.

The risk assessment for the Health Information Technology for Economic and Clinical Health Act security standards proved to be a worthwhile investment of time, energy, and money.

It provided the foundation for the risk analysis mandated for the Health Information Technology for Economic and Clinical Health Act security standards. Table 14 demonstrates 63.16% of the participants conduct a security risk assessment once every year as compared to 33.3% of the respondents in Zineddine's (2008) study.

Table 14

Frequency of Security Risk Assessment

| | Frequency | Percent | Valid Percent | Cumulative Percent |
|---------------------|-----------|---------|---------------|-----------------------|
| Only once | 6 | 31.58 | 31.58 | 31.58 |
| Once Every Year | 12 | 63.16 | 63.16 | 94.74 |
| Twice Every Year | 1 | 5.26 | 5.26 | 100 |
| Total | 19 | 100 | 100 | |

Based on the 63.16% of the hospitals conducting a risk assessment annually as shown in Table 14, it makes sense that 15.79% of the participants report implementing security measures to mitigate risks and vulnerabilities prior to the Health Insurance Portability and Accountability Act. Another 15.79% implemented measures beginning in 2005 prior to the Health Insurance Portability and Accountability Act compliance deadline as depicted in Table 15.

Table 15

Implementation of HIPAA Security Measures

| | Frequency | Percent | Valid Percent | Cumulative Percent |
|--|-----------|---------|---------------|-----------------------|
|--|-----------|---------|---------------|-----------------------|

Table 15 Implementation of HIPAA Security Measures (Continued)

| | | | | |
|------------------------|---|-------|-------|-------|
| Not Yet | 2 | 10.54 | 10.54 | 10.54 |
| 2009 | 5 | 26.32 | 26.32 | 36.87 |
| 2008 | 1 | 5.26 | 5.26 | 42.12 |
| 2007 | 3 | 15.79 | 15.79 | 57.91 |
| 2006 | 1 | 5.26 | 5.26 | 63.17 |
| 2005 | 3 | 15.79 | 15.79 | 78.96 |
| Prior to April 2005 | 3 | 15.79 | 15.79 | 94.75 |
| I Don't Know | 1 | 5.26 | 5.26 | 100 |
| Total | | 100 | 100 | |

Question 14 on the survey requests the same information as question 13 except it is specific to the Health Information Technology for Economic and Clinical Health Act security standards, and as such, the scale starts at 2008 to accommodate the Health Information Technology for Economic and Clinical Health Act security standards compliance date. Table 16 shows that 36.84% of the responding hospitals have not implemented any security measures to mitigate risks and vulnerabilities as defined in the Health Information Technology for Economic and Clinical Health Act security standards. Conversely, 42.11% of the hospitals implemented security measures in 2010 and 15.79% implemented security measures in 2009.

Table 16

Implementation of HITECH Security Measures

| | Frequency | Percent | Valid Percent | Cumulative Percent |
|--------------|-----------|---------|---------------|-----------------------|
| Not Yet | 7 | 36.84 | 36.84 | 36.84 |
| 2010 | 8 | 42.11 | 42.11 | 78.95 |
| 2009 | 3 | 15.79 | 15.79 | 94.74 |
| I Don't Know | 1 | 5.26 | 5.26 | 100 |
| Total | 19 | 100 | 100 | |

Question 15 asks, “when did your hospital implement systems/procedures to regularly review records of information system activity such as audit logs, access reports, and security incident tracking reports?” Table 17 shows that all the participants report implementation of systems and procedures to review audit logs, access reports, and security incident tracking reports after the Health Information Insurance Portability and Accountability Act compliance date of 2005.

Table 17

Audit Logs, Access Reports, and Tracking Reports

| | Frequency | Percent | Valid Percent | Cumulative Percent |
|---------|-----------|---------|---------------|-----------------------|
| Not Yet | 4 | 21.05 | 21.05 | 21.05 |
| 2009 | 4 | 21.05 | 21.05 | 42.10 |

Table 17 Audit Logs, Access Reports, and Tracking Reports (Continued)

| | | | | |
|--------------|----|-------|-------|-------|
| 2008 | 2 | 10.54 | 10.54 | 52.64 |
| 2007 | 1 | 5.26 | 5.26 | 57.90 |
| 2006 | 1 | 5.26 | 5.26 | 63.16 |
| 2005 After | 6 | 31.58 | 31.58 | 94.74 |
| HIPAA | | | | |
| I Don't Know | 1 | 5.26 | 5.26 | 100 |
| Total | 19 | 100 | 100 | |

Question 16 asks, “when did your hospital identify a security official who is responsible for the development, implementation, and updating of policy and procedures related to HIPAA?” A majority of the participants reported they had a security official in place by the Health Insurance Portability and Accountability Act compliance deadline as shown in Table 18.

Table 18

Identification of a Security Official

| | Frequency | Percent | Valid Percent | Cumulative Percent |
|---------|-----------|---------|---------------|-----------------------|
| Not Yet | 1 | 5.26 | 5.26 | 5.26 |
| 2009 | 1 | 5.26 | 5.26 | 10.52 |
| 2008 | 2 | 10.53 | 10.53 | 21.05 |
| 2006 | 2 | 10.53 | 10.53 | 31.58 |

Table 18 Identification of a Security Official (Continued)

| | | | | |
|--------------|----|-------|-------|-------|
| 2005 After | 5 | 26.32 | 26.32 | 57.90 |
| HIPAA | | | | |
| 2005 Before | 7 | 36.84 | 36.84 | 94.74 |
| HIPAA | | | | |
| I Don't Know | 1 | 5.26 | 5.26 | 100 |
| Total | 19 | 100 | 100 | |

Question 17 states, “when did your hospital implement procedures regarding workforce access and safeguarding of PHI?” As Table 19 shows, approximately 79% of the participants reported implementing access and safeguards procedures sometime after the Health Insurance Portability and Accountability Act compliance deadline.

Table 19

Implementation of Workforce Access Procedures

| | Frequency | Percent | Valid Percent | Cumulative Percent |
|------------|-----------|---------|---------------|-----------------------|
| 2009 | 1 | 5.26 | 5.26 | 5.26 |
| 2008 | 2 | 10.54 | 10.54 | 15.80 |
| 2006 | 4 | 21.05 | 21.05 | 36.85 |
| 2005 After | 8 | 42.1 | 42.1 | 78.95 |
| HIPAA | | | | |

Table 19 Implementation of Workforce Access Procedures (Continued)

| | | | | |
|--------------|----|-------|-------|-------|
| 2005 Before | 3 | 15.79 | 15.79 | 94.74 |
| HIPAA | | | | |
| I Don't Know | 1 | 5.26 | 5.26 | 100 |
| Total | 19 | 100 | 100 | |

Question 18 asks, “when did your hospital implement procedures for terminating access to PHI when employment of a workforce member ends?” Table 20 shows that 52.63% of the hospitals implemented procedures for termination of access to PHI before the Health Insurance Portability and Accountability Act compliance deadline.

Table 20

Procedures for Terminating Access to PHI

| | Frequency | Percent | Valid Percent | Cumulative Percent |
|--------------|-----------|---------|---------------|-----------------------|
| 2009 | 1 | 5.26 | 5.26 | 5.26 |
| 2008 | 1 | 5.26 | 5.26 | 10.52 |
| 2006 | 2 | 10.53 | 10.53 | 21.05 |
| 2005 After | 4 | 21.06 | 21.06 | 42.11 |
| HIPAA | | | | |
| 2005 Before | 10 | 52.63 | 52.63 | 94.74 |
| HIPAA | | | | |
| I Don't Know | 1 | 5.26 | 5.26 | 100 |

Table 20 Procedures for Terminating Access to PHI (Continued)

| | | | |
|-------|----|-----|-----|
| Total | 19 | 100 | 100 |
|-------|----|-----|-----|

Question 19 asked, “when did your hospital implement a process to determine users’ authorization and access level to protected health information?” Approximately 63% of the respondents reported having processes in place to determine their users’ authorization and level of access in 2005 of which 42.1% of the respondents reported having the processes in place prior to the compliance deadline shown in Table 21. The respondents in the Zineddine (2008) study reported 87.56% of the surveyed entities had these processes in place in 2005.

Table 21

User Authorization and Access Level to PHI

| | Frequency | Percent | Valid Percent | Cumulative Percent |
|----------------------|-----------|---------|---------------|-----------------------|
| 2009 | 2 | 10.52 | 10.52 | 10.52 |
| 2006 | 4 | 21.06 | 21.06 | 31.58 |
| 2005 After HIPAA | 4 | 21.06 | 21.06 | 52.64 |
| 2005 Before HIPAA | 8 | 42.1 | 42.1 | 94.74 |
| I Don’t Know | 1 | 5.26 | 5.26 | 100 |
| Total | 19 | 100 | 100 | |

Question 20 asked, “when did your hospital implement systems/procedures to guard against, detect, and report malicious software?” As shown in Table 22, over 60% of the respondents reported having the ability to guard against, detect, and report malicious software compared to 52.1% of the respondents in the Zineddine (2008) study.

Table 22

Ability to Guard Against, Detect, and Report Malicious Software

| | Frequency | Percent | Valid Percent | Cumulative Percent |
|----------------------|-----------|---------|---------------|-----------------------|
| 2009 | 1 | 5.26 | 5.26 | 5.26 |
| 2008 | 1 | 5.26 | 5.26 | 10.52 |
| 2006 | 4 | 21.06 | 21.06 | 31.58 |
| 2005 Before HIPAA | 12 | 63.16 | 63.16 | 94.74 |
| I Don't Know | 1 | 5.26 | 5.26 | 100 |
| Total | 19 | 100 | 100 | |

Question 21 asked, “when did your hospital implement procedures for creating, changing, and safeguarding passwords?” As shown in Table 23, over 68% of the respondents reported having procedures in place to create, change, and safeguard passwords. Surprisingly, 15.8% of the respondents stated their facilities did not implement these procedures until 2008 or later.

Table 23

Procedures to Create, Change, and Safeguard Passwords

| | Frequency | Percent | Valid Percent | Cumulative Percent |
|----------------------|-----------|---------|---------------|-----------------------|
| 2009 | 1 | 5.26 | 5.26 | 5.26 |
| 2008 | 2 | 10.54 | 10.54 | 15.8 |
| 2005 After HIPAA | 2 | 10.54 | 10.54 | 26.34 |
| 2005 Before HIPAA | 13 | 68.4 | 68.4 | 94.74 |
| I Don't Know | 1 | 5.26 | 5.26 | 100 |
| Total | 19 | 100 | 100 | |

Question 22 asked, “when did your organization implement response and reporting procedures of security violations?” Table 24 shows 26.32% of the respondents stated they had a response and reporting of security violations procedure in place prior to the Health Information Insurance Portability and Accountability Act compliance deadline.

Table 24

Response and Reporting Procedures of Security Violations

| | Frequency | Percent | Valid Percent | Cumulative Percent |
|---------|-----------|---------|---------------|-----------------------|
| Not Yet | 2 | 10.54 | 10.54 | 10.54 |

Table 24 Response and Reporting Procedures of Security Violations (Continued)

| | | | | |
|-------------|----|-------|-------|-------|
| 2009 | 2 | 10.54 | 10.54 | 21.08 |
| 2008 | 1 | 5.26 | 5.26 | 26.34 |
| 2006 | 3 | 15.76 | 15.76 | 42.10 |
| 2005After | 6 | 31.58 | 31.58 | 73.68 |
| HIPAA | | | | |
| 2005 Before | 5 | 26.32 | 26.32 | 100 |
| HIPAA | | | | |
| Total | 19 | 100 | 100 | |

Question 23 asked, “when did your hospital develop a data backup plan as suggested by Health Insurance Portability and Accountability Act?” The majority of the respondents (84.22%) reported having a data backup plan in place prior to the Health Insurance Portability and Accountability Act compliance deadline as shown in Table 25. Conversely, the respondents in the Zineddine (2008) study reported 66.7% had a data backup plan in place prior to the compliance deadline.

Table 25

Data Backup Plan

| | Frequency | Percent | Valid Percent | Cumulative Percent |
|------|-----------|---------|---------------|-----------------------|
| 2007 | 1 | 5.26 | 5.26 | 5.26 |
| 2006 | 1 | 5.26 | 5.26 | 10.52 |

Table 25 Data Backup Plan (Continued)

| | | | | |
|--------------|----|-------|-------|-------|
| 2005 Before | 16 | 84.22 | 84.22 | 94.74 |
| HIPAA | | | | |
| I Don't Know | 1 | 5.26 | 5.26 | 100 |
| Total | 19 | 100 | 100 | |

Question 24 asked, “when did your hospital develop a disaster recovery plan as suggested by the Health Insurance Portability and Accountability Act security rule?” Over 50% of the respondents reported establishing a disaster recovery plan. However, as depicted in Table 26, 31.58% of the respondents reported they do not currently have a disaster recovery plan. Only 9.4% of the respondents in the Zineddine (2008) study reported they did not have a disaster recovery plan.

Table 26

Disaster Recovery

| | Frequency | Percent | Valid Percent | Cumulative Percent |
|--------------|-----------|---------|---------------|-----------------------|
| Not Yet | 6 | 31.58 | 31.58 | 31.58 |
| 2007 | 1 | 5.26 | 5.26 | 36.84 |
| 2006 | 1 | 5.26 | 5.26 | 42.10 |
| 2005 Before | 10 | 52.64 | 52.64 | 94.74 |
| HIPAA | | | | |
| I Don't Know | 1 | 5.26 | 5.26 | 100 |

Table 26 Disaster Recovery (Continued)

| | | | |
|-------|----|-----|-----|
| Total | 19 | 100 | 100 |
|-------|----|-----|-----|

Question 25 asked, “when did your hospital implement procedures for periodic testing and revision of contingency plans?” Approximately 32% of the respondents reported they do not have procedures for periodic testing and revision of contingency plans. Approximately 16% of the respondents did not know. As shown in Table 27, only 10.54% of the respondents had procedures in place prior to the Health Insurance Portability and Accountability Act compliance deadline.

Table 27

Procedures for Testing and Revising Contingency Plans

| | Frequency | Percent | Valid Percent | Cumulative Percent |
|----------------------|-----------|---------|---------------|-----------------------|
| Not Yet | 6 | 31.58 | 31.58 | 31.58 |
| 2009 | 2 | 10.54 | 10.54 | 42.12 |
| 2008 | 1 | 5.26 | 5.26 | 47.38 |
| 2006 | 2 | 10.54 | 10.54 | 57.92 |
| 2005 After HIPAA | 3 | 15.77 | 15.77 | 73.69 |
| 2005 Before HIPAA | 2 | 10.54 | 10.54 | 84.23 |
| I Don't Know | 3 | 15.77 | 15.77 | 100 |

Table 27 Procedures for Testing and Revising Contingency Plans (Continued)

| | | | |
|-------|----|-----|-----|
| Total | 19 | 100 | 100 |
|-------|----|-----|-----|

Question asked, “when did your hospital start assessing the relative criticality of specific applications and data in support of contingency planning?” Table 28 shows only 26.32% of the respondents reported they have assessed specific applications and data in support of contingency planning before the Health Insurance Portability and Accountability Act compliance deadline. Of all the respondents surveyed, 10.53% reported they have not started assessing their applications and data and 5.26% did not know.

Table 28

Assessing Specific Applications and Data

| | Frequency | Percent | Valid Percent | Cumulative Percent |
|----------------------|-----------|---------|---------------|-----------------------|
| Not Yet | 2 | 10.54 | 10.54 | 10.54 |
| 2009 | 3 | 15.74 | 15.74 | 26.28 |
| 2008 | 2 | 10.54 | 10.54 | 36.82 |
| 2007 | 2 | 10.54 | 10.54 | 47.36 |
| 2006 | 2 | 10.54 | 10.54 | 57.90 |
| 2005 After HIPAA | 2 | 10.54 | 10.54 | 68.44 |
| 2005 Before HIPAA | 5 | 26.30 | 26.30 | 94.74 |

Table 28 Assessing Specific Applications and Data (Continued)

| | | | | |
|--------------|---|------|------|-----|
| I Don't Know | 1 | 5.26 | 5.26 | 100 |
| Total | | 100 | 100 | |

Question 27 asked, “when did your hospital put in place business associate agreements ensuring that PHI will be appropriately safeguarded?” Table 29 shows that approximately 69% of the respondents had their business associate agreements in place prior to the Health Insurance Portability and Accountability Act compliance deadline in 2005. These results correlate closely to the 65.5% reported in Zineddine’s (2008) study.

Table 29

Business Associate Agreements in Place

| | Frequency | Percent | Valid Percent | Cumulative Percent |
|----------------------|-----------|---------|---------------|-----------------------|
| 2009 | 2 | 10.54 | 10.54 | 10.54 |
| 2006 | 3 | 15.78 | 15.78 | 26.32 |
| 2005 After HIPAA | 10 | 52.64 | 52.64 | 78.96 |
| 2005 Before HIPAA | 3 | 15.78 | 15.78 | 94.74 |
| I Don't Know | 1 | 5.26 | 5.26 | 100 |
| Total | 19 | 100 | 100 | |

Question 28 asked, “has your hospital updated its business associate agreements to be HITECH compliant?” The Health Information Technology for Economic and Clinical Health Act security standards mandate a specific update to the Health Insurance Portability and Accountability Act business associate agreements. Table 30 shows 78.96% of the respondents inserted the update into their business associate agreements. Of note, only 18 of the participants responded to the question. Three of the respondents or 15.74% have not updated their business associate agreements.

Table 30

Updated Business Associate Agreement to Comply With HITECH

| | Frequency | Percent | Valid Percent | Cumulative Percent |
|-------|-----------|---------|---------------|-----------------------|
| Yes | 15 | 78.96 | 78.96 | 78.96 |
| No | 3 | 15.74 | 15.74 | 100 |
| Total | 18 | 100 | 100 | |

Question 29 asked, “when did your hospital implement policies and procedures to safeguard information systems from unauthorized access, tampering, and theft?” Table 31 shows that approximately 57% of the respondents reported having policies and procedures in place to safeguard information systems from unauthorized access, tampering, and theft in 2005 compared to the 65.6% reported in Zineddine’s (2008) study. That said 10.54% did not implement the policies and procedures until 2009.

Table 31

Safeguard Systems

| | Frequency | Percent | Valid Percent | Cumulative Percent |
|--------------|-----------|---------|---------------|-----------------------|
| 2009 | 2 | 10.54 | 10.54 | 10.54 |
| 2008 | 1 | 5.26 | 5.26 | 15.80 |
| 2007 | 1 | 5.26 | 5.26 | 21.06 |
| 2006 | 3 | 15.79 | 15.79 | 36.85 |
| 2005 After | 4 | 21.05 | 21.05 | 57.90 |
| HIPAA | | | | |
| 2005 Before | 7 | 36.84 | 36.84 | 94.74 |
| HIPAA | | | | |
| I Don't Know | 1 | 5.26 | 5.26 | 100 |
| Total | 19 | 100 | 100 | |

Question 30 asked, “when did your hospital implement physical safeguards for workstations that access PHI, restricting access to authorized users?” Over 58% of the respondents reported having physical safeguards in place for workstations accessing protected health information as shown in Table 32. This correlated closely to the 50% reported in Zineddine’s (2008) study. One respondent or 5.26% reported they do not have any physical safeguards in place and another 5.26% reported they did not know if their organization had any safeguards in place.

Table 32

Physical Safeguards for Workstations Accessing PHI

| | Frequency | Percent | Valid Percent | Cumulative Percent |
|----------------------|-----------|---------|---------------|-----------------------|
| Not Yet | 1 | 5.26 | 5.26 | 5.26 |
| 2008 | 2 | 10.54 | 10.54 | 15.80 |
| 2006 | 4 | 21.04 | 21.04 | 36.84 |
| 2005 After HIPAA | 6 | 31.58 | 31.58 | 68.42 |
| 2005 Before HIPAA | 5 | 26.32 | 26.32 | 94.74 |
| I Don't Know | 1 | 5.26 | 5.26 | 100 |
| Total | 19 | 100 | 100 | |

Question 31 asked, “when did your hospital implement a mechanism to encrypt and decrypt electronic media containing PHI?” Table 33 shows 36.84% of the respondents reported they have not implemented a mechanism to encrypt or decrypt electronic media containing protected health information. Only 5.26% of the respondents reported having a mechanism in place prior to the Health Insurance Portability and Accountability Act compliance deadline.

Table 33

Encrypt and Decrypt

| | Frequency | Percent | Valid Percent | Cumulative Percent |
|-----------------------|-----------|---------|---------------|-----------------------|
| Not Yet | 7 | 36.84 | 36.84 | 36.84 |
| 2009 | 5 | 26.32 | 26.32 | 63.16 |
| 2008 | 2 | 10.54 | 10.54 | 73.70 |
| 2005 After | 3 | 15.78 | 15.78 | 89.48 |
| HIPAA 2005 Before | 1 | 5.26 | 5.26 | 94.74 |
| HIPAA I Don't Know | 1 | 5.26 | 5.26 | 100 |
| Total | | 100 | 100 | |

Survey question 32 asked, “when did your hospital implement security measures to ensure that electronically transmitted information is protected against unauthorized modification until it is disposed of?” Only 26.32% of the respondents reported they have security measures in place to protect electronically transmitted information against unauthorized modification before the Health Insurance Portability and Accountability Act compliance deadline. Another 21.04% of the respondents reported they did not know and 26.30% reported they have not implemented these security measures yet as shown in Table 34. The 26.30% correlates extremely closely to the 29.2% reported in the Zineddine (2008) study.

Table 34

Security Measures for Electronically Transmitted Information

| | Frequency | Percent | Valid Percent | Cumulative Percent |
|--------------|-----------|---------|---------------|-----------------------|
| Not Yet | 5 | 26.30 | 26.30 | 26.30 |
| 2009 | 2 | 10.54 | 10.54 | 36.84 |
| 2008 | 2 | 10.54 | 10.54 | 47.38 |
| 2007 | 1 | 5.26 | 5.26 | 52.64 |
| 2005 After | 3 | 15.78 | 15.78 | 68.42 |
| HIPAA | | | | |
| 2005 Before | 2 | 10.54 | 10.54 | 78.96 |
| HIPAA | | | | |
| I Don't Know | 4 | 21.04 | 21.04 | 100 |
| Total | 19 | 100 | 100 | |

Question 33 asked, “has your hospital updated its policies and procedures for breach of process and accounting of disclosures?” The majority of the respondents; 78.94% reported having policies and procedures in place for accounting of disclosures as shown in Table 35.

Table 35

Accounting of Disclosures

| | Frequency | Percent | Valid Percent | Cumulative Percent |
|--|-----------|---------|---------------|-----------------------|
|--|-----------|---------|---------------|-----------------------|

Table 35 Accounting of Disclosures (Continued)

| | | | | |
|-------|----|-------|-------|-------|
| Yes | 15 | 78.94 | 78.94 | 78.94 |
| No | 4 | 21.06 | 21.06 | 100 |
| Total | 19 | 100 | 100 | |

Question 34 asked, “to what degree are the following factors challenges to the implementation of the HIPAA, HITECH, and Red Flag security standards?” Table 36 shows the ten challenges from the survey questionnaire ranked by their statistical mean. When ranked by the mean, cost came in last. This was an opposite finding in Zineddine’s (2008) study. When ranked by mean, cost and complexity ranked highest. Conversely, 47.36% of the respondents reported cost and the complexity of the rules as being the biggest challenges to the implementation of the security standards. Approximately 33% of the respondents identified the lack of effective leadership as the most benign challenge.

Table 36

Security Standard Implementation Challenges Ranked by Mean

| Challenge | Rank | N | Mean | Std. Deviation |
|---------------------------------|------|----|------|----------------|
| Lack of Interest | 1 | 18 | 3.83 | 1.043 |
| Absence of Effective Leadership | 2 | 18 | 3.83 | 1.150 |
| Lack of Expertise in Security | 3 | 18 | 3.78 | 1.060 |

Table 36 Security Standard Implementation Challenges Ranked by Mean (Continued)

| | | | | |
|-------------------|----|----|------|-------|
| Lack of Expertise | 4 | 18 | 3.67 | .970 |
| in HITECH and | | | | |
| Red Flag | | | | |
| Standards | | | | |
| Absence of | 5 | 18 | 3.61 | .916 |
| Official | | | | |
| Certification | | | | |
| Process | | | | |
| Lack of Expertise | 6 | 18 | 3.50 | 1.150 |
| Misunderstanding | 7 | 18 | 3.11 | .900 |
| Ambiguity | 8 | 18 | 3.06 | .802 |
| Complexity of | 9 | 18 | 2.61 | 1.092 |
| the Rules | | | | |
| Cost | 10 | 18 | 2.56 | 1.042 |

Question 35 asked, “to be compliant with both Red Flag Rules and HITECH Standards, your hospital intends to do or has already done which of the following?” An overwhelming 94.74% of the respondents reported they plan to change or have already changed policies and procedures to detect and block security breaches. Only 68.42% of the respondents reported they would make additional investments in security tools and technologies. Approximately 89% of

the respondents reported they would revise security policies and procedures and 84% would provide additional training for staff.

Question 36 asked, “to the best of my knowledge, my hospital is fully compliant with the HIPAA, HITECH, and Red Flag standards.” Shown in Table 37; 57.90% of the respondents reported they agreed that they are fully compliant with all standards while 36.84% of the respondents did not agree or disagree.

Table 37

Fully Complaint with HIPAA, HITECH, and Red Flag Standards

| | Frequency | Percent | Valid Percent | Cumulative Percent |
|------------------------------|-----------|---------|---------------|-----------------------|
| Agree | 11 | 57.90 | 57.90 | 57.90 |
| Neither Agree or Disagree | 7 | 36.84 | 36.84 | 94.74 |
| Disagree | 1 | 5.26 | 5.26 | 100 |
| Total | 19 | 100 | 100 | |

Question 37 asked, “how difficult is it to comply with multiple, government mandated initiatives in a relatively short period?” Table 38 shows 47.36% of the respondents report it is very difficult to comply with multiple government mandates in a relatively short period.

Table 38

Difficulty Complying with Multiple Government Mandates

| | Frequency | Percent | Valid Percent | Cumulative Percent |
|------------------------|-----------|---------|---------------|-----------------------|
| Somewhat Difficult | 5 | 26.32 | | 26.32 |
| Very Difficult | 9 | 47.36 | | 73.68 |
| Extremely Difficult | 5 | 26.32 | | 100 |
| Total | 19 | 100 | 100 | |

Question 38 asked, “on 7/14/2010 the Office for Civil Rights released the required risk analysis requirements under the security rule. Has your hospital complied with the risk analysis requirement?” As shown in Table 39; 63.14% of the respondents reported they were only somewhat compliant while 26.32% reported they have not started the analysis.

Table 39

Compliance with Risk Analysis Requirement

| | Frequency | Percent | Valid Percent | Cumulative Percent |
|-----------------|-----------|---------|---------------|-----------------------|
| Fully Compliant | 2 | 10.54 | 10.54 | 10.54 |

Table 39 Compliance with Risk Analysis Requirement (Continued)

| | | | | |
|-----------------|----|-------|-------|-------|
| Somewhat | 12 | 63.14 | 63.14 | 73.68 |
| Compliant | | | | |
| Haven't Started | 5 | 26.32 | 26.32 | 100 |
| Yet | | | | |
| Total | 19 | 100 | 100 | |

The final survey question asked, “is your hospital actively pursuing the "meaningful use" incentives issued by Medicare and Medicaid Services to become a meaningful user of certified electronic health record technology?” Every responded (100%) reported they were actively pursuing meaningful use certification.

Chapter 5 - Discussion

Conclusions

As stated earlier, the study lacks statistical significance relative to the low number of survey responses, therefore; the writer is unable to make any definitive conclusions from the research. Moreover, the research raised more questions than it answered which the writer discusses in the next chapter. That said, the writer did note several themes and trends during the analysis of the data in which the writer will use as a bases to discuss the research questions.

Research question one asked “what effect did the mandate have on compliance?” The data strongly suggests that a government mandate in and of itself; is not enough to force a hospital to comply. The writer introduced survey questions 13, 15 through 27, and 29 through 32 specifically to determine the level of compliance achieved with the Health Insurance Portability and Accountability Act. Questions 13, 15, 16, 22, 24, 25, 26, 30, 31, and all contained responses

in the “Not Yet” category meaning; they have not complied with a specific Health Insurance Portability and Accountability Act standard the question related to. Most telling included questions 24 and 25 where 32% of the respondents reported they had not implemented a disaster recovery plan or any procedures for testing and making revisions to their contingency plans. Question 31 showed that approximately 37% of the respondents have not implemented a mechanism for encrypting and decrypting electronic media containing protected health information. At a minimum, these responses suggest that six years after the Health Insurance Portability and Accountability Act compliance deadline, hospitals are not fully compliant.

The suggestion that hospitals are not fully compliant correlates well with the results of Zineddine’s (2008) study. The data itself correlates but not necessarily closely. The writer expected less correlation over time. As technology advanced and in many cases became cheaper, some hospitals likely embraced technology that brought them into compliance. Additionally, with the new government mandates issued, many hospitals realized to comply with the new mandates; organizations would need to be in compliance with the Health Insurance Portability and Accountability Act.

Research question two asked, “what effect did complying with multiple mandates over time have on the healthcare organization?” The data shows that 47.36% of the respondents stated complying with multiple government mandates was “very difficult” and 26.32% of the respondents reported it was “extremely difficult.” Survey question 14 shows 36.84% of the respondents have not implemented the security measures as defined in the Health Information Technology for Economic and Clinical Health Act and Red Flag Rules standards. The data suggests that complying with multiple government mandated statutes concerning security of protected health information and information systems is more difficult than trying to comply

with a single government mandate. The writer points out that the data merely suggests and does not prove this theory. It is possible that other factors may exist.

Research question three asked, “what effect did cost have on compliance?” The survey shows 31.58% of the respondents rated cost as a “High” challenge to achieving compliance and 15.78% of the respondents rated cost as a “Very High” challenge to achieving compliance. Conversely, when the writer ranked all of the listed challenges by their statistical mean, “cost” ranked in last place. Clearly, 47.36% of the respondents perceived “cost” as a significant challenge. The data as presented is unable to quantify what role cost played in level of compliance achieved.

Research question four asked, “was cost the only constraint to compliance, or was there other challenges such as hospital size, geographical location and perception or interpretation of the standards?” The survey showed 15.78% of the respondents rated the complexity of the rules as being a “Very High” challenge to compliance and 31.58 reported complexity as a “High” challenge to compliance. Approximately 56% of the respondents reported ambiguity of the standards and misunderstanding of the standards as a “Moderate” challenge to achieving compliance. Approximately 39% of the respondents reported lack of interest in compliance at a minimum; a “Moderate” challenge to achieving compliance. “Ambiguity,” “Misunderstanding,” “Absence of an official certification process,” “Lack of interest,” “Cost, Lack of expertise in security,” “Absence of effective leadership,” “Complexity of the rules,” “Lack of expertise in HIPAA security,” and “Lack of expertise in HITECH and Red Flag Rules” standards all created challenges to achieving compliance. However, the writer is unable to quantify how big or how little of a challenge each of these data elements was.

Research question five asked, “what impact did compliance have on the security of electronic patient information?” Asked another way, “does a government mandated regulation achieve the intended outcome?” The data suggests that in many cases hospitals have not achieved full compliance. Failing to achieve full compliance suggests the intended outcome of a government mandated regulation is irrelevant.

Zineddine (2008) argued the need for government mandated regulations suggesting compliance would be less than it currently is. Voluntary compliance in and of itself he suggests, would not be enough to get hospitals to fully comply. This writer doesn’t feel the data in Zineddine’s study supports his assertion. Zineddine’s assertion is likely an opinion and not based on fact.

Survey question 39 asked,” is your hospital actively pursuing the "meaningful use" incentives issued by Medicare and Medicaid Services to become a meaningful user of certified electronic health record technology?” Every respondent (100%) reported their organization is actively pursuing “Meaningful Use” certification. The writer believes the response to this question is a significant statement in that most hospitals that successfully meet the criteria in the allotted timeframe will receive incentive money ranging from one million dollars to more than six million dollars over a four-year period. On the surface, it suggests that when organizations are appropriately incented, they are more likely to comply.

The writer believes government mandated regulations should use both a carrot and stick approach when issuing a mandated regulation. Based on the responses to survey question 39, financial incentives seem to work as a motivator. While one cannot conclude that the financial incentive will mean all hospitals will achieve compliance with the “Meaningful Use” standards,

the data reported in this survey suggests the hospitals are well intended and in the early stages of attempting to meet the “meaningful use” standards; the 100% positive response is impressive.

Study Limitations

This study has several limitations identified by the writer of which the poor response rate is the most concerning. The poor response rate, (less than four percent) despite sending out 600 invitations to participate in the study presented a substantial limitation. The poor response rate has rendered the study statistically insignificant. Several factors likely contributed to the poor response. Of those factors, sending out the invitations during the Christmas holiday is likely a key contributor to the poor response rate. Unfortunately, due to the university deadlines, delaying the study was not an option.

The writer used the United States postal system to mail the invitation and consent form to potential participants. In many cases, the name of the Information Technology department director or manager was unknown and a generic mailing label was created and used as opposed to some other medium or database with the appropriate mailing information. Generic letters can be lost, discarded, and misplaced after opened. Additionally, the writer was unable to send potential participants a reminder letter due to cost constraints and concerns that the second letter had the same probability of getting to the recipient as the first letter did.

The purchase of a database specific targeting Information Technology directors or managers that contained both mailing addresses and e-mail addresses may have increased the probability of a higher response rate. The database would provide a direct means of communication and the ability to provide follow up correspondence such as a reminder e-mail.

Early in the study design; the writer made the decision to use survey questions from an existing study. The writer did not anticipate any difficulties in establishing contact with the

author of the chosen study and therefore; did not build in any contingencies in the study timeline. The author of the chosen study, Mhamed Zineddine, PhD left the country and went back to Dubai. Tracking the author to Dubai and getting the necessary permission to use his survey questions took much longer than expected. The extra time spent meant the study was mailed as a “pilot study” and survey questions reliability and validity would be verified upon receipt of the participants’ responses. This process is an acceptable practice however; it likely compromised the survey question design by not affording the writer the ability to redesign the questions if the validity and reliability became a concern.

Several of the survey questions proved to be a limitation of the study. The writer used too many questions focused on the Health Insurance Portability and Accountability Act to determine the current level of compliance achieved by each hospital. In retrospect, the writer should have created “drill down” questions to look at the “why” as well as the “what.” The subject of cost is a perfect example. The study as conducted identified cost as playing a role in achieving compliance however, the questions regarding cost did not afford the writer the opportunity to determine the role it played and what affect it had on compliance.

Another technical limitation was, the writer did not anticipate difficulties with document editing and as such did not consider the use of an editor. It became self evident that when a writer spends excessive time in a lengthy document; cognitive pattern recognition becomes an issue; leading the writer to believe elements of a sentence exist when in fact they do not. Ultimately, the writer consulted an editor.

Despite several study limitations, the writer believes the study merits further consideration from others contemplating research in the area of government mandated regulations. Health care costs are skyrocketing and the subject of many debates among

politicians. The cost of implementation of various government mandates ultimately get passed on the consumer hence the practice of “cost shifting.” That said, the acronym ARRA, American Recovery and Reinvestment Act of 2009, the act responsible for the Health Information Technology for Economic and Clinical Health Act, is an oxymoron. It seeks to cut and control costs but in reality, it likely contributes to the costs it professes to control. If the premise of the study could be quantified, perhaps the lawmakers would be more thoughtful before they sign an act into law.

References

- American Health Information Management Association (AHIMA). "The State of HIPAA Privacy and Security Compliance 2005." Chicago: AHIMA, 2005, Retrieved October 20, 2010 from:
http://library.ahima.org/xpedio/groups/public/documents/ahima/pub_bok1_026502.html
- Arora, R., & Pimentel, M. (2005). Cost of privacy: A HIPAA perspective. (Ed.). Pittsburg, PA: Carnegie Mellon University.
- ARRA and HITECH Legislation. (2011). Retrieved on April 7, 2011 from American Health Information Management Association:
<http://www.ahima.org/advocacy/arralegislationregulation.aspx>
- Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). A model for evaluating IT security investments. *Communications of the ACM*, 47, 87-92.
- Choudhury, A. (2010). *Cronbach's Alpha*. Retrieved April 5, 2011 from Experiment Resources:
<http://www.experiment-resources.com/cronbachs-alpha.html#ixzz1J3xPfsv1>
- Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2nd edition). Hillsdale, NJ: Erlbaum.
- Creswell, J. W. (2009). *Research design: qualitative, quantitative, and mixed methods*. (3rd ed.). Thousand Oaks, CA: Sage Publications. ISBN: 1412965578
- Department of Health and Human Services. (2002). *45 CFR Parts 160 and 164, Standards for Privacy of Individually Identifiable Health Information*. Washington D.C.: National Archives and Records Administration.
- Department of Health and Human Services, Office of the Secretary, Part II 45 CFR Parts 160, 162, and 164, Health Insurance Reform: Security Standards, *Federal Register* / February 20, 2003, Washington D.C.: National Archives and Records Administration.
- Department of Health and Human Services, Office of the Secretary, Part II, 45 CFR Parts 160 HIPAA Administrative Simplification: Enforcement, Summary, *Federal Register* / Vol. 71, No. 32, / February 16, 2006 / Rules and Regulations.
- Department of Health and Human Services, Office of the Secretary, Part II, 45 CFR Parts 160, 162, and 164, "I. Background, A. Statutory Background", *Federal Register* / Vol. 68, / February 16, 2006 / Rules and Regulations.
- Department of Treasury, Office of the Comptroller of the Currency, Part IV, 12 CFR Part 41, Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003, *Federal Register* / Vol. 72, No. 217, / November 9, 2007, / Rules and Regulations.

References (Continued)

- Department of Treasury, Office of Thrift Supervision, Part IV, 12 CFR Part 571, Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003, *Federal Register* / Vol. 72, No. 217, / November 9, 2007, / Rules and Regulations.
- Economic Stimulus: The HITECH Act of 2009*. (2010). Retrieved June 25, 2010 from IMPAC Medical Systems Inc.: <http://www.impac.com/hitech-act.html>.
- EHR Incentive Program: Eligible Hospital and CAH Meaningful Use Table of Contents Core Objectives and Menu Set Objectives*. (2010). Retrieved on April 7, 2011 from Centers for Medicare and Medicaid Services (CMS): http://www.cms.gov/EHRIncentivePrograms/Downloads/Hosp_CAH_MU-TOC.pdf
- Fast facts on US hospitals*, (2009). Retrieved March 12, 2011 from American Hospital Association: <http://www.aha.org>
- Federal Deposit Insurance Corporation, Part IV, 12 CFR Part 222, Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003, *Federal Register* / Vol. 72, No. 217, / November 9, 2007, / Rules and Regulations.
- Federal Reserve System, Part IV, 12 CFR Parts 334 and 364 Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003, *Federal Register* / Vol. 72, No. 217, / November 9, 2007, / Rules and Regulations.
- Federal Trade Commission, Part IV, 16 CFR Part 681, Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003, *Federal Register* / Vol. 72, No. 217, / November 9, 2007, / Rules and Regulations.
- Gay, L. R., Mills, G. E., & Airasian, P. (2009). *Educational research: Competencies for analysis and application* (9th ed.). Upper Saddle River, NJ: Merrill/Pearson Education.
- Having, K. & Davis, D C. (2005). HIPAA compliance in U.S. hospitals: A self report of progress towards the security rule. *Perspectives in Health Information Management*. 2;9 Fall 2009.
- Health Care, The American Heritage Medical Dictionary*. (2007). Retrieved April 7, 2011 from The Free Dictionary: <http://medical-dictionary.thefreedictionary.com/health+care>
- HIPAA compliance: Cost-effective solutions for the technical security regulations*. (2001). Retrieved June 25, 2010 from SANS Institute Infosec Reading Room: <http://www.sansinstitute.com>.

References (Continued)

HIPAA cost considerations, (2003). Retrieved June 23, 2010 from Health Data Management: <http://www.healthdatamanagement.com>.

Internet usage statistics, the internet big picture, (2010). Retrieved March 10, 2011 from Internet World Stats: [http:// www.internetworldstats.com/stats.htm](http://www.internetworldstats.com/stats.htm)

Leedy, P. D., & Ormrod, J. E. (2010). *Practical research: Planning and design* (9th ed.). New York: Merrill/Prentice Hall (Pearson Education). ISBN: 978-0-13-715242-1 or 0-13-715242-6 soft.

Lowry, R. (2011). *Concepts & Applications of Inferential Statistics*. Vassar College, Poughkeepsie, NY, USA. Retrieved April 5, 2011 from Vassar College: <http://faculty.vassar.edu/lowry/ch4pt1.html>

Mail surveys vs. web surveys: A comparison, (2007). Retrieved March 3, 2011 from Super Survey: <http://knowledge-base.supersurvey.com/mail-vs-web-surveys.htm>

National Credit Union Administration, Part IV, 12 CFR Part 717, Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003, *Federal Register* / Vol. 72, No. 217, / November 9, 2007, / Rules and Regulations.

Public Law 104-191 Health Insurance Portability and Accountability Act of 1996. (2004). Retrieved June 28, 2010 from U.S. Department of Health & Human Services: <http://aspe.hhs.gov/adminsimp/p1104191.htm>.

Shuttleworth, M. (2009). *Definition of Reliability*. Retrieved April 5, 2011 from Experiment Resources: <http://www.experiment-resources.com/Definition-of-reliability.html#ixzz1J3yOIBIL>

Stigler, S. (2008). *Fisher and the 5% level*. *Chance* **21** (4): 12, Springer, New York, December 1, 2008. Retrieved April 5, 2011, from <http://dx.doi.org/10.1007/s00144-008-0033-3>

Thornton, G. (2009). *Red flags rule: What healthcare businesses need to know*. Retrieved June 25, 2010 from Grant Thornton LLP: <http://www.grantthornton.com>.

Upton, G., & Cook, I. (2006). *Oxford Dictionary of Statistics*, (2nd Edition), OUP. [ISBN 978-0-19-954145-4](http://www.oxfordjournals.org/doi/abs/10.1093/acprof:oso/9780199541454)

Zineddine, M. (2008). Compliance of the healthcare industry with the Health Insurance Portability and Accountability Act security regulations in Washington State: A quantitative study two years after mandatory compliance. Capella University 2008.

Appendix A

1. CONSENT TO PARTICIPATE IN RESEARCH I have read the "consent to participate in this research survey" document provided to me in the letter of introduction. By clicking the "I Accept" button below I acknowledge I understand the information provided to me regarding this study and voluntarily agree to participate in the research by answering the following survey questions.
 - a. I accept
 - b. I decline
2. The hospital I work for is:
 - a. ☐ For profit
 - b. ☐ Not for profit
3. The hospital zip code is:

4. The total number of hospital beds are:
 - a. ☐ 5 – 50
 - b. ☐ 51 – 100
 - c. ☐ 101 – 200
 - d. ☐ 201 – 300
 - e. ☐ 301 – 400
 - f. ☐ 401 – 500
 - g. ☐ > 501
5. Total number of employees in the IT department?
 - a. ☐ 1-10
 - b. ☐ 11-20
 - c. ☐ 21-50
 - d. ☐ 51-100
 - e. ☐ > 100
6. How many years have you been employed at this hospital?

7. What is the highest level of education you have completed?
 - a. ☐ High School/GED
 - b. ☐ Some College
 - c. ☐ 2-Year College Degree (Associates)
 - d. ☐ 4-Year College Degree (BA, BS)
 - e. ☐ Master's Degree
 - f. ☐ Doctoral Degree

- g. ☐ Professional Degree (MD, JD)
 - h. ☐ Other
8. How knowledgeable are you about the HIPAA Security Rule?
- a. ☐ Very Knowledgeable
 - b. ☐ Somewhat Knowledgeable
 - c. ☐ Not Knowledgeable
9. How knowledgeable are you about the HITECH Security Standards?
- a. ☐ Very Knowledgeable
 - b. ☐ Somewhat Knowledgeable
 - c. ☐ Not Knowledgeable
10. How knowledgeable are you about the Red Flag Rules?
- a. ☐ Very Knowledgeable
 - b. ☐ Somewhat Knowledgeable
 - c. ☐ Not Knowledgeable
11. In which of the following years has your hospital allocated a specific budget to gain information and for the ongoing management of the security program? (Choose all that apply)
- a. ☐ 2010
 - b. ☐ 2009
 - c. ☐ 2008
 - d. ☐ 2007
 - e. ☐ 2006
 - f. ☐ 2005
 - g. ☐ 2004
 - h. ☐ 2003
 - i. ☐ No Budget
 - j. ☐ Don't Know
12. My hospital conducts a thorough IT risk assessment to determine potential risks that may threaten the security of PHI.
- a. ☐ Never
 - b. ☐ Only Once
 - c. ☐ Once a Year
 - d. ☐ Twice a Year
 - e. ☐ 3 or More Times a Year
 - f. ☐ I don't Know
 - g. ☐ Yes but not driven by HIPAA, HITECH, or the Red Flag Rules

13. When did your hospital implement security measures sufficient to mitigate risks and vulnerabilities to a reasonable and appropriate level as defined in the final HIPAA security rule?
- a. ☐ Not yet
 - b. ☐ 2009
 - c. ☐ 2008
 - d. ☐ 2007
 - e. ☐ 2006
 - f. ☐ 2005
 - g. ☐ Prior to April 2005
 - h. ☐ I don't know
14. When did your hospital implement security measures sufficient to mitigate risks and vulnerabilities to a reasonable and appropriate level as defined in the final HITEC security rule and Red Flag Rules?
- a. ☐ Not yet
 - b. ☐ 2010
 - c. ☐ 2009
 - d. ☐ 2008
 - e. ☐ I don't know
15. When did your hospital implement systems/procedures to regularly review records of information system activity such as audit logs, access reports, and security incident tracking reports?
- a. ☐ Not yet
 - b. ☐ 2009
 - c. ☐ 2008
 - d. ☐ 2007
 - e. ☐ 2006
 - f. ☐ 2005 after HIPAA
 - g. ☐ 2005 before HIPAA
 - h. ☐ I don't know
16. When did your hospital identify a security official who is responsible for the development, implementation, and updating of policy and procedures related to HIPAA?
- a. ☐ Not yet
 - b. ☐ 2009
 - c. ☐ 2008
 - d. ☐ 2007
 - e. ☐ 2006
 - f. ☐ 2005 after HIPAA
 - g. ☐ 2005 before HIPAA
 - h. ☐ I don't know
17. When did your hospital identify a security official who is responsible for the development, implementation, and updating of policy and procedures related to HIPAA?

- a. ☐ Not yet
 - b. ☐ 2010
 - c. ☐ 2009
 - d. ☐ 2008
 - e. ☐ 2007
 - f. ☐ 2006
 - g. ☐ 2005 after HIPAA
 - h. ☐ 2005 before HIPAA
 - i. ☐ I don't know
18. When did your hospital implement procedures regarding workforce access and safeguarding of PHI?
- a. ☐ Not yet
 - b. ☐ 2009
 - c. ☐ 2008
 - d. ☐ 2007
 - e. ☐ 2006
 - f. ☐ 2005 after HIPAA
 - g. ☐ 2005 before HIPAA
 - h. ☐ I don't know
19. When did your hospital implement procedures for terminating access to PHI when employment of a workforce member ends?
- a. ☐ Not yet
 - b. ☐ 2009
 - c. ☐ 2008
 - d. ☐ 2007
 - e. ☐ 2006
 - f. ☐ 2005 after HIPAA
 - g. ☐ 2005 before HIPAA
 - h. ☐ I don't know
20. When did your hospital implement a process to determine users' authorization and access level to PHI?
- a. ☐ Not yet
 - b. ☐ 2009
 - c. ☐ 2008
 - d. ☐ 2007
 - e. ☐ 2006
 - f. ☐ 2005 after HIPAA
 - g. ☐ 2005 before HIPAA
 - h. ☐ I don't know
21. When did your hospital implement systems/procedures to guard against, detect, and report malicious software?

- a. ☐ Not yet
 - b. ☐ 2009
 - c. ☐ 2008
 - d. ☐ 2007
 - e. ☐ 2006
 - f. ☐ 2005 after HIPAA
 - g. ☐ 2005 before HIPAA
 - h. ☐ I don't know
22. When did your hospital implement procedures for creating, changing, and safeguarding passwords?
- a. ☐ Not yet
 - b. ☐ 2009
 - c. ☐ 2008
 - d. ☐ 2007
 - e. ☐ 2006
 - f. ☐ 2005 after HIPAA
 - g. ☐ 2005 before HIPAA
 - h. ☐ I don't know
23. When did your organization implement response and reporting procedures of security violations?
- a. ☐ Not yet
 - b. ☐ 2009
 - c. ☐ 2008
 - d. ☐ 2007
 - e. ☐ 2006
 - f. ☐ 2005 after HIPAA
 - g. ☐ 2005 before HIPAA
 - h. ☐ I don't know
24. When did your hospital develop a data backup plan as suggested by HIPAA?
- a. ☐ Not yet
 - b. ☐ 2009
 - c. ☐ 2008
 - d. ☐ 2007
 - e. ☐ 2006
 - f. ☐ 2005 after HIPAA
 - g. ☐ 2005 before HIPAA
 - h. ☐ I don't know
25. When did your hospital develop a disaster recovery plan as suggested by the HIPAA security rule?
- i. ☐ Not yet
 - j. ☐ 2009
 - k. ☐ 2008

- l. ☐ 2007
 - m. ☐ 2006
 - n. ☐ 2005 after HIPAA
 - o. ☐ 2005 before HIPAA
 - p. ☐ I don't know
26. When did your hospital implement procedures for periodic testing and revision of contingency plans?
- q. ☐ Not yet
 - r. ☐ 2009
 - s. ☐ 2008
 - t. ☐ 2007
 - u. ☐ 2006
 - v. ☐ 2005 after HIPAA
 - w. ☐ 2005 before HIPAA
 - x. ☐ I don't know
27. When did your hospital start assessing the relative criticality of specific applications and data in support of contingency plan component?
- a. ☐ Not yet
 - b. ☐ 2009
 - c. ☐ 2008
 - d. ☐ 2007
 - e. ☐ 2006
 - f. ☐ 2005 after HIPAA
 - g. ☐ 2005 before HIPAA
 - h. ☐ I don't know
28. When did your hospital put in place business associate agreements ensuring that PHI will be appropriately safeguarded?
- a. ☐ Not yet
 - b. ☐ 2009
 - c. ☐ 2008
 - d. ☐ 2007
 - e. ☐ 2006
 - f. ☐ 2005 after HIPAA
 - g. ☐ 2005 before HIPAA
 - h. ☐ I don't know
29. Has your hospital updated its business associate agreements to be HITECH compliant?
- a. ☐ Yes
 - b. ☐ No
30. When did your hospital implement policies and procedures to safeguard information systems from unauthorized access, tampering, and theft?
- a. ☐ Not yet

- b. ☐ 2009
 - c. ☐ 2008
 - d. ☐ 2007
 - e. ☐ 2006
 - f. ☐ 2005 after HIPAA
 - g. ☐ 2005 before HIPAA
 - h. ☐ I don't know
31. When did your hospital implement physical safeguards for workstations that access PHI, restricting access to authorized users?
- a. ☐ Not yet
 - b. ☐ 2009
 - c. ☐ 2008
 - d. ☐ 2007
 - e. ☐ 2006
 - f. ☐ 2005 after HIPAA
 - g. ☐ 2005 before HIPAA
 - h. ☐ I don't know
32. When did your hospital implement a mechanism to encrypt and decrypt electronic media containing PHI?
- a. ☐ Not yet
 - b. ☐ 2009
 - c. ☐ 2008
 - d. ☐ 2007
 - e. ☐ 2006
 - f. ☐ 2005 after HIPAA
 - g. ☐ 2005 before HIPAA
 - h. ☐ I don't know
33. When did your hospital implement security measures to ensure that electronically transmitted information is protected against unauthorized modification until it is disposed of?
- a. ☐ Not yet
 - b. ☐ 2009
 - c. ☐ 2008
 - d. ☐ 2007
 - e. ☐ 2006
 - f. ☐ 2005 after HIPAA
 - g. ☐ 2005 before HIPAA
 - h. ☐ I don't know
34. Has your hospital updated its policies and procedures for breach of process and accounting of disclosures?
- a. ☐ Yes
 - b. ☐ No

35. To what degree are the following factors challenges to the implementation of the HIPAA, HITEC, and Red Flag Rule security standards?

| | Very Highly | Highly | Moderately | Somewhat | Not at all |
|--|-------------|--------|------------|----------|------------|
| Ambiguity | | | | | |
| Misunderstanding | | | | | |
| Absence of an Official certification process | | | | | |
| Lack of interest in compliance | | | | | |
| Cost | | | | | |
| Lack of expertise in security | | | | | |
| Absence of effective leadership | | | | | |
| Complexity of the rules | | | | | |
| Lack of expertise in HIPAA Security rule | | | | | |
| Lack of expertise in HITECH & Red Flag Rules | | | | | |

36. To be compliant with both Red Flag Rules and HITECH Standards, your hospital intends to do or has already done which of the following? (Pick all that apply)

- a. ☐ Change policies and procedures to prevent/detect data breaches
- b. ☐ Provide additional training for staff
- c. ☐ Revise security policies and procedures
- d. ☐ Make additional investments in security tools/technologies

37. To the best of my knowledge, my hospital is fully compliant with the HIPAA, HITECH, and Red Flag standards.

- a. ☐ Strongly Agree
- b. ☐ Agree
- c. ☐ Neither Agree or Disagree
- d. ☐ Disagree
- e. ☐ Strongly Disagree

38. How difficult is it to comply with multiple, government mandated initiatives in a relatively short period?

- a. ☐ Not Difficult
- b. ☐ Somewhat Difficult

- c. ☐ Very Difficult
 - d. ☐ Extremely Difficult
39. On 7/14/2010, the Office for Civil Rights released the required risk analysis requirements under the security rule. Has your hospital complied with the risk analysis requirement?
- a. ☐ Fully compliant
 - b. ☐ Somewhat compliant
 - c. ☐ Not compliant
 - d. ☐ Haven't started yet
40. Is your hospital actively perusing the "meaningful use" incentives issued by Medicare and Medicaid Services to become a meaningful user of certified electronic health record technology?
- a. ☐ Yes
 - b. ☐ No

Appendix B

Title of Study:

Mandated Government Regulations in Healthcare: Is Healthcare IT Overregulated?

Principle Investigator:

Name: Mark Albright

University: Regis University

Department of: School of Computer and Information Sciences

Address: 3333 Regis Blvd., Denver, CO 80221-1099

Phone: (719) 650-5585

E-mail: albri820@regis.edu

Advisor: Dr. Ed Lindoo

CONSENT TO PARTICIPATE IN RESEARCH

Background:

You have been selected to participate in this research study. Before you decide to participate, it is important that you understand why the study is being done, the procedures, the benefits, the risks and discomforts, and all precautions taken. Please read all of the following information carefully. After you read the following information, if there is anything that is not clear or you need further information, please contact me at the phone number or e-mail address listed above.

Purpose of this study is to determine if healthcare IT organizations are over regulated by analyzing the following questions:

7. What effect did the mandate have on compliance?
8. What effect did complying with multiple mandates over time have on the healthcare organization?
9. What effect did cost have on compliance?
10. Was cost the only constraint to compliance or were there other challenges such as hospital size, geographical location and perception or interpretation of the standards?
11. What impact did compliance have on the security of electronic patient information?

Study Procedure:

You will be asked to complete an on-line survey consisting of 38 questions of which most are multiple choice type questions at the following URL: <http://www.zoomerang.com/Survey/WEB22BK84D3P4Q/>

Question #1 is a disclaimer stating that you have read this document and you give your consent to participate in this study by clicking on the "Accept" button. You will not be able to submit your survey without accepting the terms of this consent. If you "Accept" you will be able to complete most of the survey questions by clicking on the answer you intend to provide. Other answers allow for insertion of free text. When completed, you will be prompted to click on the "Submit" button. The survey should take no more than 15-20 minutes of your time.

Risks/Discomforts:

There are no foreseeable risks or discomforts to you for participating in this study.

Benefits:

Although there will be no direct benefit to you for participating in this study, the study will provide information where information either does not exist or is proprietary and not met for public review. It will begin to determine if the authors of federal statutes are realizing the desired outcomes of the regulations. Because the body of knowledge regarding this subject matter is so limited, this study will provide a basis for future researchers to provide contributions, thereby growing the body of knowledge and perhaps having a future effect on regulatory proposals and IT departments.

Alternative Procedures:

There are no alternative procedures necessary for this study.

Confidentiality:

During the participant selection process, some demographical information was collected. This information included your hospital's name, address, phone number, website URL, your name, phone number and e-mail address. Your confidentiality and your hospital's confidentiality will be protected at all times. No demographical information listed above will be used in any reports or publications. This information will be kept separate from the study information under lock and key. Only this writer will have access to that information. At the end of the study, the demographic information will be destroyed.

Study Withdrawal:

The decision to take part in this study is completely voluntary. You do not have to participate. Even if you decide at first to participate, you are free to change your mind at any time and quit the study. Your decision to withdrawal from the study will not affect my grade for this study or my status as a student.

Costs:

There are no costs to you to participate in this study.

Compensation:

There is no monetary compensation to you for participating in this study.

Questions and Concerns:

If you have questions about this research, please contact this writer at (719) 650-5585 or albri820@regis.edu. You may also contact the faculty member supervising this work: Dr. Ed Lindoo, ed.lindoo@scripps.com

Signature:

By clicking the "accept" button on the on-line survey you acknowledge that you understand the information given to you in this form and that you voluntarily agree to participate in the research described above.

Appendix C

December 5, 2010

Subject: Thesis Survey

Dear IT Director/Manager,

My name is Mark Albright; I am a graduate student at Regis University in the School of Computer and Information Sciences. I am currently writing my thesis, a requirement to complete my Master's degree in Systems Engineering.

My research tool is an on-line survey that asks questions about compliance with HIPAA Security Standards, HITECH Security Standards, and the Red Flag Rules. It should take no more than 15-20 minutes of your time. I would greatly appreciate it if you would read the enclosed consent document and then fill out the survey located at:

<http://www.zoomerang.com/Survey/WEB22BK84D3P4Q/>

I thank you in advance for your time and participation, Thank You!

Sincerely,
Mark Albright