Fall 12-1-2014

A Case Study of Information System Security Compliance Of Small Medical and Dental Practices

Debra Landry Folse
Indiana State University

A CASE STUDY OF INFORMATION SYSTEM SECURITY COMPLIANCE OF SMALL MEDICAL AND DENTAL PRACTICES

A Dissertation

Presented to

College of Graduate and Professional Studies

College of Technology

Indiana State University

Terre Haute, Indiana

In Partial Fulfillment

of the Requirements for the Degree

Doctor of Philosophy

---

by

Debra Landry Folse

December 2014

VITA

Debra Landry Folse

EDUCATION

Ph.D.	Indiana State University, Terre Haute, IN. Technology Management, 2014.
MSCIS	University of South Alabama, Mobile, AL. Computer Information Sciences, 2000.
MBA	Southeastern Louisiana University, Hammond, LA. Business Administration, 1991.
B.A.	Southeastern Louisiana University, Hammond, LA. Marketing, 1989.

PROFESSIONAL EXPERIENCE

2003 – 2006	Instructor – Department of Marketing & E-Commerce, Mitchell College of Business, University of South Alabama, Mobile, Alabama.
1999 – 2002	Instructor / Network Administrator - Department of Management, Mitchell College of Business, University of South Alabama, Mobile, Alabama.

PUBLICATIONS

Folse, D.L., (2007, May) "The Application of Sensor-Based Wireless Networks in Supply Chain Management", ISA District 12: Proceedings of the International Forum. "Information Systems, Problems, Perspectives, Innovation Approaches", Student Competition. St. Petersburg, Russia. Vol. 2.

Folse, D.L., Longenecker, H.E., & Daigle, R.J., (2003, November) "Influence of Covey Habit Training on Teams", Journal of Information Systems Education, Vol. 1, Issue No. 54.

COMMITTEE MEMBERS

Committee Chair: Dr. Gerald W. Cockrell

Professor Emeritus, Retired

Indiana State University

Committee Member: Dr. David P. Beach

Professor, Retired

Indiana State University

Committee Member: Dr. Eileen D. Seeman

Associate Professor, Department of Management Information Systems

East Carolina University

ABSTRACT

Small medical and dental practices must comply with the Health Insurance Portability and Accountability Act (HIPAA) of 1996, and Title XIII Health Information Technology for Economic and Clinical Health (HITECH) of the American Recovery and Reinvestment Act (ARRA) of 2009. The case study, utilizing interviews, observations, and existing documentation of two medical and the two dental practices, not only analyzed the compliance solution choices made involving procedures and technologies, but also analyzed the emotion aspects of fear of non-compliance, perceived confidence in compliance, and the primary and secondary appraisals of the compelled compliance. Although compliance is not an easy process, small medical and dental practices can discover a number of possible options and identify the best fit solution for their practice in the effort to affect compliance.

ACKNOWLEDGEMENTS

The dissertation was a very lengthy and arduous process containing many high points but far more low points; however, the thought of abandoning the effort was inconceivable. In the final analysis, it was an incredible learning experience on multiple levels.

I would like to thank my committee for their shear fortitude on my behalf. Dr. Gerald W. Cockrell, my chair, has been the perfect blend of a hard taskmaster, a wise confidant, and a compassionate friend. Dr. David P. Beach has been my crucial devil's advocate. His astute comments and suggestions have guided me into discovering and appreciating new insights not only in the field of research but also within myself. "Thank you, Dr. Beach!" Dr. Elaine D. Seeman has graciously shared her knowledge, experience, and expertise to ensure that my concepts were fully articulated. Also, I would like to thank Mary (Mebby) Griffy for her conscientiousness in providing to me the necessary and timely information throughout the entire process.

I must thank God for giving me the ability to accomplish this task and to continue to pursue "Debra's Great Adventure". To my mother and father, Anna Leahy Landry and Joseph Landry who expected great deeds from me, to work hard, and to never give up. To my wonderful husband, James, who is the love of my life and my life's facilitator.

TABLE OF CONTENTS

LIST OF TABLES

CHAPTER 1

INTRODUCTION

On the United States Department of Health and Human Services' (HHS) website is the "Wall of Shame" where healthcare data breaches by the offending entities are posted as reported by articles in Modern Healthcare and Healthcare Informatics. (Conn, 2013; DeGaspari, 2012) In an effort to reduce the number of security breaches and to assure compliance to federal mandates, HHS has started conducting audits of a number of healthcare providers each year. In a report dated November, 2013 the Department of Health and Human Services Office of Inspector General stated in the Executive Summary based on the May 2011 report, "We recommended that OCR [Office of Civil Rights] continue the compliance audit process that CMS [Centers for Medicare and Medicaid Services] had begun and implement procedures for conducting compliance audits to ensure that Security Rule controls are in place and operating as intended to protect ePHI [electronic Protected Health Information] at covered entities." (Salmon, 2013 p. i) Additionally, in a 2013 memorandum to the Assistant Inspector General for Audit Services at the Department of Health and Human Services from the Director of the Office of Civil Rights, the office currently responsible for the oversight and enforcement of the Security Rule and which is included as Appendix B in the November 2013 report, stated that "the audit results demonstrated several clear trends……small [covered] entities overall struggled in each assessment area-privacy, security and breach notification-while larger entities had proportionally fewer and more limited findings." (Rodriguez, 2013 p. 4) Small medical and dental practices are included in the small "covered entities" designation by the Department of Health and Human Services as

identified in the Health Information Portability and Accountability Act (HIPAA). (HIPAA, 1996) A component of HIPAA, the Security Rule, mandates that electronic protected health information (ePHI) be secure. However, HIPAA did not state penalties for non-compliance. Included in the 2009 American Recovery and Reinvestment Act is Title XIII-The Health Information Technology for Economic and Clinical Health (HITECH) which outlines the penalties for non-compliance of the Security Rule and breach notification requirements. (ARRA, 2009; HIPAA, 1996)

The Centers for Medicare and Medicaid Services (CMS) created a series of documents which are intended to guide the groups covered under the Security Rule to accomplish compliance. Medical and dental offices are included in the "covered entities" group and are required to comply. The goal of the Security Rule is to secure electronic protected health information (ePHI) that is created, modified, stored, and transmitted. According to CMS, "The process should, at a minimum, require covered entities to: 1) assess current security, risks, and gaps, and 2) develop an implementation plan." ("HIPAA Security 101 for Covered Entities", 2007, p. 6) The series of documents cover the security standards for the administrative, physical, and technical aspects along with the organizations' policies, procedures, and documents required. In addition to the above standards, the concept of risk analysis and management are included in the series. ("HIPAA Basics of Risk Analysis and Risk Management", 2007)

The CMS Technical Security Safeguards are defined as "the technology and the policy and procedures for its use that protect electronic protected health information and control access to it." ("HIPAA Security Standards Technical Safeguards", 2007, p. 2) These technical

safeguards include access control, audit controls, integrity, person or entity authentication, and transmission security. (“HIPAA Security Standards Technical Safeguards”, 2007)

The CMS Physical Security Safeguards are defined as “the physical measures, policies and procedures to protect electronic information systems, buildings and equipment”. (“HIPAA Security Standards Physical Safeguards”, 2007, p. 13) The physical safeguards include facility access controls, workstation use, workstation security, and device and media controls.

The CMS Administrative Security Safeguards include security management process, assignment security responsibility, workforce security, information access management, security awareness and training, security incident procedures, contingency plan, evaluation, and business associate contracts and other arrangements. (“HIPAA Security Standards Administrative Safeguards”, 2007)

In addition to the CMS HIPAA Security Standards Series, the National Institute of Standards and Technology (NIST) created a group of Special Publications (SP) that are available and useful to the general public. The list for SP800 publications is quite lengthy and covers various security situations. Specifically, SP800-66 “An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule”, and SP800-30 “Risk Analysis and Management” are helpful documents for compliance along with the NIST HIPAA Security Rule (HSR) Toolkit. (“HSR Toolkit”, 2011, Scholl, et al., 2008; Stoneburner, Goguen, & Feringa, 2002).

One of the CMS Security Series documents covers the basics of risk analysis and management. This document along with NIST SP 800-30 Risk Analysis and Management are valuable resources in the compliance process. The compliance process, as directed by CMS,

should entail assessing security, risk, and gaps. ("HIPAA Security 101 for Covered Entities", 2007) Assessing vulnerability is a first step in the risk analysis and management process. To assure the security of the electronic protected health information (ePHI) residing within their systems and to attain federal compliance, healthcare providers should assess their vulnerabilities. By limiting the number of vulnerabilities within a system, the opportunity for hackers to gain access and for data to be breached may be reduced. (Scarfone, et.al, 2008) The research project focus included aspects of the Administrative, Physical, and Technical Security Safeguards along with the vulnerability assessment aspect of the Risk Analysis and Management Process. "HIPAA ("HIPAA Security Standards Administrative Safeguards", 2007; ("HIPAA Security Standards Physical Safeguards", 2007; "HIPAA Security Standards Technical Safeguards", 2007; Basics of Risk Analysis and Risk Management", 2007)

The assessment for vulnerability involves not only the technology but also the people and the procedures. The process for assessing the technological vulnerabilities is to search for weaknesses within the information system. (Clifford, 2004; Volonino & Robinson, 2004) Assessing the vulnerabilities regarding procedures involve the analysis of the organization's security policies and practices.

The final component of vulnerability assessment concerns the people involved. In the study the focus was the physicians' and dentists' and their staffs' emotions or personal reactions and actions regarding IS security compliance. Journal articles covering information system security, compliance, and use have considered the emotions of users in their research. (Kwon & Johnson, 2013; Beaudry & Pinsonneault, 2010; Johnston & Warkentin, 2010; Beaudry & Pinsonneault, 2005)

According to recent National Science Foundation grant funded research by Eric Johnson, Dean of the Owen Graduate School of Management at Vanderbilt University, and Juhee Kwon, assistant professor in the Information Systems Department at College of Business City University of Hong Kong, reported that the threat or fear of non-compliance is the driving force behind security efforts in non-mature organizations securing electronic patient information. (Kwon & Johnson, 2013) Additionally the Kwon and Johnson study referenced the research by Allen Johnston and Merrill Warkentin. Dr. Johnston is an assistant professor at the University of Alabama Birmingham and received his Ph.D. in Information Systems from Mississippi State University. One focus of his primary research is on the behavioral aspects of information security and privacy. Dr. Merrill Warkentin is Professor of MIS and the John and Carole Ferguson Notable Scholar at Mississippi State University. Also, he is the Department Editor of IS Security & Privacy for the Association for Information Systems and the next chair of the International Federation for Information Processing (IFIP) Working Group on Information Systems Security Research. Their article, "Fear Appeals and Information Security Behaviors: An Empirical Study" studied the fear component. (Johnson & Warkentin, 2010) The result of the Johnson and Warkentin study on the fear element indicated that users view technology as a means to lessen security threats above the need for security performance advancement.

In their articles, "The Other Side of Acceptance: Studying the Direct and Indirect Effects of Emotions on Information Technology Use" in 2010 and their prior article "Understanding User Responses to Information Technology: A Coping Model of User Adaption" in 2005, Anne Beaudry and Alain Pinsonneault studied the effects of user's emotions on information technology use. (Beaudry & Pinsonneault, 2010; Beaudry & Pinsonneault, 2005) In their 2005

article, the researchers state that an IT event triggers a coping mechanism. The primary appraisal by the user will view the event as either an opportunity or a threat. The secondary appraisal is based on whether the user perceives they have control over the event or no control over the event. The combination of the primary and secondary appraisals by the user would indicate an adaptation strategy of Benefits Satisficing (opportunity/no control), Benefits Maximizing (opportunity/control), Disturbance Handling (threat/control) or Self-Preservation (threat/no control). (Beaudry & Pinsonneault, 2005)

In their 2010 article, the researchers took the same basic premise of opportunity or threat as the primary appraisal and user perceived control or no control as the secondary appraisal to classify emotions. The combination of the primary and secondary appraisals by the user would indicate an emotion classification as Achievement Emotions (opportunity/no control), Challenge Emotions (opportunity/control), Deterrence Emotions (threat/control) or Loss Emotions (threat/no control). In dealing with the emotion classifications, the authors listed a number of emotions within each category. Within the Achievement Emotions (opportunity/no control) are happiness, satisfaction, pleasure, relief, and enjoyment and within the Challenge Emotions (opportunity/control) are excitement, hope, anticipation, arousal, playfulness, and flow. Within the Deterrence Emotions (threat/control) are anxiety, fear, worry, and distress and within the Loss Emotions (threat/no control) are anger, dissatisfaction, disappointment, annoyed, frustration, and disgust. (Beaudry & Pinsonneault, 2010) However, the authors only studied the first emotion in each category. The research study utilized Beaudry's and Pinsonneault's Framework for Classifying Emotions to categorize where the physicians and dentists placed based on their primary and secondary appraisals of compelled security compliance.

General Statement of the Problem

The US Department of Health and Human Services is conducting audits to test compliance to the HIPAA Security Rule by covered entities. Small medical and dental practices may not be in compliance with the Security Rule. Their financial resources and technical expertise may be insufficient regarding "what to do" and "how to do it". These practices may have a perception of compliance by checking the boxes in a form rather than in providing the necessary security measures. Compelled compliance with the Security Rule may generate primary and secondary appraisals by physicians and dentists that may impact their emotions and actions regarding the situation. The research study focused on acquiring an understanding of existing perceptions, emotions, practices and procedures involved in attaining security compliance. The level of understanding provided the ability to identify commonalities and differences in the medical and dental practices, along with trends that highlight small covered entities' security compliance issues and to add to the current body of knowledge.

The Purpose Statement

The purpose of the case study was to understand, describe, and discover the current state of information system security compliance of two medical and two dental practices based on an assessment of vulnerability. The proposed assessment included the people, the procedures, and the technology involved in security compliance. The reasoning for selecting two different types of healthcare providers was to compare and to identify commonalities and differences, and to discover possible trends. It was a conjecture that since the medical offices and area hospitals share patient information, the medical offices were not only better informed than dental offices

as to the importance of compliance and information system security practices but also more fearful of the repercussions for non-compliance.

Research Questions

The Central Question:

How compliant to the Security Rule of HIPAA and secure are information systems in the small medical and dental practices?

Sub-Questions:

Question 1 – How do the medical and dental practices assess the security of their information systems regarding identifying possible vulnerabilities?

Question 2 – How are security practices and internal system controls implemented?

Question 3 – How confident are the physicians and dentists regarding their "perceived" compliance with the HIPAA Security Rule?

Question 4 – How does the physicians' and dentists' fear of non-compliance influence security compliance?

Question 5 – How do the physicians' and dentists' primary and secondary appraisals to compelled compliance influence security compliance?

Question 6 – How do security compliance decisions differ in medical and dental practices?

Significance of Study

Compliance with the federal mandates assures that electronic protected health information when created, modified, stored, and transmitted is secure. The idea that patient information could be accessed and made public is a concern and data breaches are expected to increase. Security compliance decisions by small medical and dental practices are influenced by

the technology, the procedures, and the people involved. Factors such as technical expertise, financial resources, perceptions and emotions along with the primary and secondary appraisals of the compelled compliance may influence the implementation of the components and procedures necessary to achieve security compliance. The research study purported that the knowledge gained by an understanding of the physicians', dentists' and their staff's procedural and technical issues along with their perceptions and emotions concerning compelled compliance was helpful to other small healthcare providers, and medical and dental students by identifying commonalities, differences, and trends.

Limitations

Only medical and dental practices located within the United States could be included in this study since the federal law mandates of HIPAA and ARRA/HITECH only pertain to the United States.

Only medical and dental practices using Electronic Health Records (EHR) in their facilities are affected by the federal mandates of HIPAA Security Rule and ARRA/HITECH.

HIPAA security standards and guidelines will be utilized as the basis for analyzing compliance.

Due to resource constraints of time and distance, only small medical and dental practices located within the southern gulf coast region of the states of Alabama, Louisiana, and Mississippi, and the northern gulf coast region of the state of Florida will be considered in this study.

Definition of Terms

The US Department of Health and Human Services (HHS) – The federal agency responsible for the oversight and enforcement of the Security Rule of the Health Insurance Portability and Accountability Act of 1996.

Electronic Health Record (EHR) – contains the information regarding a patient from a number of service provider sources such as the primary physician, lab reports, pharmacy documents and other contributing medical specialists services along with hospital services.

Electronic Protected Health Information (ePHI) – individually identifiable health information in electronic form.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) – a United States of America Federal Law.

The Health Information Technology for Economic and Clinical Health (HITECH) Title XIII of the American Recovery and Reinvestment Act (ARRA) of 2009 – a United States of America Federal Law.

National Institute of Standards and Technology (NIST) – the entity responsible for creating standards and guidelines to ensure proper information system security for all governmental agencies except national security systems.

Risk Analysis and Management - the process that requires information system vulnerabilities be identified, analyzed, and handle based on the organizations determination of impact to the security of the information system and its selected level of risk.

System Vulnerabilities – deficiencies within an information system that would allow for possible attack to the system.

CHAPTER 2

LITERATURE REVIEW

Overview

The United States Federal Government enacted the Health Insurance Portability and Accountability Act (HIPAA) in 1996. (HIPAA, 1996) Contained within HIPAA is the Security Rule which covers specific required standards implementation specifications and addressable implementation specifications meant to provide the necessary security of electronic protected health information (ePHI). (HIPAA, 1996) The governmental agency responsible for the enforcement of HIPAA is the Department of Health and Human Services (HHS). Originally, HHS gave the administration and enforcement of the Security Rule to the Centers of Medicare and Medicaid Services (CMS) unit within HHS. Currently, the Office of Civil Rights (OCR) within HHS is responsible for the administration and enforcement of the Security Rule. The CMS developed and distributed a series of documents covering specific safeguards to be used as guidelines for assuring security compliance. ("HIPAA Security Standards Series", 2007)

The administrative safeguards include security management process, assignment security responsibility, workforce security, information access management, security awareness and training, security incident procedures, contingency plan, evaluation, and business associate contracts and other arrangements. ("HIPAA Security Standards Administrative Safeguards", 2007) The physical safeguards include facility access controls, workstation use, workstation

security, and device and media controls. (“HIPAA Security Standards Physical Safeguards”, 2007)

The technical safeguards include access control, audit controls, integrity, person or entity authentication, and transmission security. (“HIPAA Security Standards Technical Safeguards”, 2007) Access control allows only those individuals or programs to utilize information systems, resources, programs, or data. Audit controls monitor the activities of information system users, information systems, resources, programs, or data to insure proper use and functionality. Integrity means that information systems, resources, programs, or data has not been accidentally or maliciously altered or deleted. Person or entity authentication uses various techniques that verify that a person or entity is who they present themselves to be. Transmission security means that the information is secure from any tampering while in transit. (“HIPAA Security Technical Standards”, 2007)

To ensure the security of electronic protected health information and to assure that healthcare organizations are in compliance to HIPAA, the Health Information Technology for Economic and Clinical Health (HITECH) Title XIII of the American Recovery and Reinvestment Act (ARRA) was mandated in 2009. (ARRA, 2009) HITECH has renewed fervor in the healthcare industry to comply with HIPAA by stipulating penalties for non-compliance and security breaches. (ARRA, 2009)

To facilitate information systems’ compliance to the numerous regulations to which various federal agencies shall comply, the U.S. Federal Government has given the National Institute of Standards and Technology (NIST) this role. NIST has prepared numerous Special Publications for governmental agencies to follow in securing the various information systems in

use by the Federal government. These Special Publications are available and recommended to the public for securing information systems and for assuring security compliance. The listing for the SP800 series of publications is quite lengthy and covers many specific security situations.

Healthcare Security Issues

As early as 1997, one year after HIPAA became a regulation, Thomas Rindfleisch, director of the Lane Medical Library and director for the Center for Advanced Medical Informatics at Stanford University, suggested information system security problems would exist within the healthcare industry. (Rindfleisch, 1997) One of the common concerns involving healthcare security was the topic of an article titled, "Securing ePHI" in which the differing views on security and security implementation between IT personnel and healthcare providers were explored in an academic medical center setting. The results of the study indicated that security could be improved by conducting specialized training where both the IT staff and clinical personal were involved in the development of the programs. This was based on the results of their study that indicated clinical personnel better assimilated "situational" rather than "theoretical" examples of the security issues. (Stevenson & Valenta, 2009) Dr. Stevenson is a Clinical Assistant Professor, Biomedical and Health Information Sciences at the University of Illinois - Chicago. He is a researcher, professor and security professional. He teaches Health Care Networks, Information Security and Q Methodology and is a reviewer for Program Committee for ACM International Health Informatics Symposium (IHI). Dr. Stevenson has been in the data and telecommunication for over twenty-five years and received his security certification from $(ISC)^2$. Dr. Annette Valenta is professor and Associate Dean for Health Information and Technology in the College of Applied Health Sciences at the University of

Illinois – Chicago where she was asked to develop UIC's model curriculum in informatics: the first national federally funded graduate-level specialization in health informatics and information management.

Compliance Requirements

One of the major requirements for compliance with HIPAA is that the risk analysis and management process shall be incorporated into a healthcare organizations' documentation. (Stoneburner, Goguen, & Feringa, 2002; HIPAA, 1996) The risk analysis and management process requires that vulnerabilities shall be identified, analyzed, and the proper action taken to handle the vulnerability based on the organizations determination of impact to the security of the information system and the organizations' selected level of risk. ("HIPAA Basics of Risk Analysis and Risk Management", 2007; Stoneburner, Goguen, & Feringa, 2002) Vulnerability identification is the first step in the risk analysis and management process.

Vulnerability assessment is the process of identifying vulnerabilities and the assessment should include the people and the procedures along with the technology. The technology component of vulnerability assessment involves the information system's hardware, software, applications, network, and communications components. The procedures component involves the security policies, plans, and procedures along with training practices to ensure that the established policies and procedures are adequate, in effect, and are enforced. There are a number of organizations which publish guidelines and governance activities regarding the management of information system security and compliance such as NIST, the International Information Systems Security Certification Consortium, Inc. $(ISC)^2$, and the Information System Audit and Control Association (ISACA) to name a few. (Sewart, Tittel & Chapple, 2011)

Emotion Aspect

The people component involves the owners, administrators, and users of the system. The physicians, dentists and their staffs are the people assessment for the research study. Since a reason for securing electronic protected health information is federal compliance with HIPAA, the physicians' and dentists' emotions will be included in the study. In their 2005 article, "Understanding User Responses to Information Technology: A Coping Model of User Adaptation", Beaudry and Pinsonneault looked at user adaption strategies using a framework that placed users into a four quadrant diagram based on responses to a primary appraisal of viewing an IT event as an opportunity or threat and a secondary appraisal of the user having control or no control over the IT event. (Beaudry & Pinsonneault, 2005) The Opportunity/No Control quadrant is labeled the Benefits Satisficing Strategy where the adaptation efforts by the user will be minor and insignificant, the Opportunity/Control quadrant is labeled the Benefits Maximizing Strategy where the adaptation efforts by the user will be broad and far reaching, the Threat/Control quadrant is labeled the Disturbance Handling Strategy where the adaptation efforts are self-satisfying, and the Threat/No Control quadrant is labeled the Self-Preservation Strategy where the adaptation efforts will be avoidance or non-existent.

Anne Beaudry's and Alain Pinsonneault's Framework for Classifying Emotions in their article, "The Other Side of Acceptance: Studying the Direct and Indirect Effects of Emotions on Information Technology Use", categorizes where users fall based on their primary and secondary appraisals of an IT event. In dealing with the emotion classifications, the authors listed a number of emotions within each category. Within the Achievement Emotions (opportunity/no control) are happiness, satisfaction, pleasure, relief, and enjoyment and within the Challenge Emotions

(opportunity/control) are excitement, hope, anticipation, arousal, playfulness, and flow. Within the Deterrence Emotions (threat/control) are anxiety, fear, worry, and distress and within the Loss Emotions (threat/no control) are anger, dissatisfaction, disappointment, annoyed, frustration, and disgust. (Beaudry & Pinsonneault, 2010) Anne Beaudry is an associate professor at the John Molson School of Business, Concordia University. She earned her Ph.D. at HEC Montréal. Her research focuses on IT-related user behaviors and reactions and on impacts of IT use. Alain Pinsonneault is a James McGill Professor and the Imasco Chair of Information Systems in the Desautels Faculty of Management at McGill University. His research interests include the organizational and individual impacts of information technology, user adaptation, ERP implementation, e-health, and e-integration. Both Beaudry and Pinsonneault have published in numerous journals including MIS Quarterly, Information Systems Research, and the Journal of MIS.

In the article, "Fear Appeals and Information Security Behaviors: An Empirical Study", the fear component was analyzed. (Johnson & Warkentin, 2010) The result of the Johnson and Warkentin study on the fear element indicated that users view technology as a means to lessen security threats above the need for security performance advancement. Additionally, in the article, "Healthcare Security Strategies for Data Protection and Regulatory Compliance", Juhee Kwon and M. Eric Johnson referenced Johnson and Warkentin and considered the aspect of fear in their research regarding non-compliance. The authors studied 243 hospitals regarding how the issues of compliance and security performance affect one another. Results of their research indicated that, "… operationally immature organizations are more likely to be motivated by compliance than actual security". (Kwon & Johnson, 2013 p. 41) Although the authors looked

at hospitals in their study, the small healthcare practices could be viewed as an operationally immature organization especially regarding EHR and IT security and as such the practices are more likely to be motivated by compliance than actual security as the Kwon and Johnson study found. The authors referenced the Capability Maturity Model (CMM) and the Privacy Maturity Model (PMM) in measuring organizational maturity. "There are five levels in the PMM that include level 1 - ad hoc, level 2 - repeatable, level 3 - defined, level 4 - managed, and level 5 - optimized. The study viewed levels 1, 2, & 3 as immature and levels 4 & 5 as mature." (Kwon & Johnson, 2013 p.45)

In the article "Future Directions for Behavioral Information Security Research", the authors identified "improving information security compliance" as one of the topics on which to focus. (Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M., & Baskerville, R., 2013 p.93) The two senior authors of the article are Dr. Merrill Warkentin and Dr. Richard Baskerville. Dr. Merrill Warkentin is Professor of MIS and the John and Carole Ferguson Notable Scholar at Mississippi State University. Additionally, he is the Department Editor of IS Security & Privacy for the Association for Information Systems and the next chair of the International Federation for Information Processing (IFIP) Working Group on Information Systems Security Research.

CHAPTER 3

METHODOLOGY

Case Study Research Approach

The case study approach fit the research study because its objective is to gain detailed knowledge and understanding, and was appropriate due to the fact that it was a collective or multiple case study analyzing and comparing four (4) subject cases. (Creswell, 2013) Another reason for selecting the case study approach has the ability to incorporate multiple data sources such as interviews, observations, and existing documentation. (Yin, 2014) The decision to include four (4) cases in this study was based on John Creswell's suggestion that five cases was the maximum number for in-depth investigations. (Creswell, 2013) Based on the facts that the study involves four cases and included several data sources to ascertain an in-depth view and eventual comparison of the perceptions, practices, and processes utilized by the case subjects in securing their information systems to be in compliance with HIPAA/HITECH, the decision was made to use the case study approach.

Goal, Strategy, and Rational for the Case Study

Goal

The goal of the case study was to not only understand and describe the conditions existing within the four case subjects, but also to discover commonalities and differences that may apply in a more generalize body of knowledge. (Yin, 2014) The knowledge gained by an

in-depth understanding of the physicians' and dentists' perceptions, emotions, procedures, and technical issues may be helpful to other small healthcare providers and to medical and dental students by identifying and highlighting commonalities, differences, and trends.

Strategy

The strategy of the case study followed the multiple case, single unit of analysis, within case, and cross case strategy by gathering data from four practices from two different segments within the healthcare industry and comparing the findings. (Creswell, 2013) The single unit of analysis concept refers to the fact that the same focus was followed for each case site under study. In the study, single unit of analysis was the operationalization of IT security within the small healthcare practices for compliance with HIPAA/HITECH. The same set of rules and procedures were followed at each case site. By the very nature of comparison, the study was a collective or multiple case structure involving more than one case site. The within case strategy used was the data analysis and representation for the case study as outlined by John Creswell. (Creswell, 2013) The strategy allowed the researcher to discover and to understand the case by letting the collected data come together and form a picture or a snapshot of the situation. The cross case strategy was used because the case study involved multiple cases. It provided a mechanism to analyze the individual cases as a combined view. This combined view allowed for the discovery of common themes and contrasting issues among the individual cases. (Yin, 2014; Creswell, 2013)

Rational

Qualitative research has been utilized and supported in numerous management information systems studies by scholarly authors for decades. In their 2012 article, "Making Successful Security Decisions: A Qualitative Evaluation", James Pettigrew III, chief of the Technical Services Division for the Chief Information Security Officer in the National Geospatial-Intelligence Agency's Office of the Chief Information Officer, and Julie Ryan, Associate Professor and Chair of George Washington University's Department of Engineering Management and Systems Engineering, used qualitative research because in their words, "Qualitative research, as opposed to quantitative research, is especially suited for exploring questions to discover and understand a subject's view of the world. You can also use it to discover processes in complex scenarios, which is a good description of the decision environment IT security managers face." (Pettigrew & Ryan, 2012, p. 60) Their article also included a sidebar detailing a number of citations related to the use of qualitative security research. In the previously cited 2013 article, "Future Directions for Behavior Information Security Research", the authors suggest that "Qualitative methodologies … could provide an effective method to better understand the actual motivations and behaviors of the insiders", and that "…studies based on qualitative methodologies such as … case studies have started to emerge in Behavioral InfoSec research." (Crossler, et.al., 2013) Merrill Warkentin, previously profiled and co-author in the above article, has utilized qualitative approaches in many of his MIS articles. Michael D. Myers, section editor on Qualitative Research in Information Systems in the Association for Information Systems Journal, stated in the updated version of his original article entitled, "Qualitative Research in Information Systems" that "Case study research is the most common qualitative method in IS". (Myers, 2013) Another author, Bonnie Kaplan, has

written numerous articles, books, and book chapters. Her research includes evaluating information systems in healthcare, approaches to healthcare information technologies, and research in information systems among others. Dr. Kaplan along with Dr. Joseph Maxwell wrote the article, "Qualitative Research Methods for Evaluating Computer Information Systems". (Kaplan & Maxwell, 1994)

In his 2009 article, "Quantified Security is a Weak Hypothesis", Verendal, then a doctoral candidate in the Department of Computer Science and Engineering at the Chalmers University, Sweden, conducted an extensive review of ninety (90) articles dated between 1981 and 2008 to ascertain if security can be presented in quantifiable terms. The result of his extensive analysis was that the quantitative work in his study was not validated. This was due to the absence of replicated studies based on the various suggested quantitative models. (Verendal, 2009).

Site Selection, Population Selection, and Sampling

The healthcare providers selected for this study were two medical practices and two dental practices. These providers were under the mandate of the Security Rule of HIPAA and HITECH covering securing electronic protected health information. The selection criteria for these practices consisted of a one or two physician/dentist office. The researcher in this study contacted potential sites by mail, email, and phone to ascertain if they were receptive and suitable to participate in the study. The medical practices and the dental practices contacted were located within the Gulf Coast region of the states of Alabama, Louisiana, and Mississippi, and the northern Gulf Coast region of the state of Florida.

Empirical Material Collection Methods

A number of data collection methods were utilized.

- An in-depth open ended interview and open question interview were conducted with the physician/dentist and their staff to ascertain the current security compliance status. Questions to determine vulnerability assessment involving the people, the procedures, and the technology were culled from the CMS HIPAA security standards for administrative, physical, and technical safeguards and the NIST HIPAA Security Rule (HSR) Toolkit. Additionally questions intended to categorize emotions relating to compelled compliance were a component of the interview. The Framework for Classifying Emotions based on elements from Beaudry's and Pinsonneault's Coping Model of User Adaption and the Effects of Emotions on Information Technology Use were incorporated to ascertain primary and secondary appraisals by physicians/dentists on compelled compliance. (Beaudry & Pinsonneault, 2010; Beaudry & Pinsonneault, 2005)

- Documents were viewed where possible that substantiated past and current security activities such as risk analysis and security policies and procedures. The document selection list was constructed from the CMS HIPAA security standards for administrative, physical, and technical safeguards and the NIST HIPAA Security Rule (HSR) Toolkit.

- The researcher conducted observations concerning the general setting of each case, the apparent physical security of the office and information system, and the system's users' security practices such as written and posted passwords, etc. Specific observational items

were obtained from the CMS HIPAA security standards for administrative, physical, and technical safeguards and the NIST HIPAA Security Rule (HSR) Toolkit.

- No protected patient information was accessed, printed, or viewed by this researcher.

Empirical Material Analysis Strategy

The analysis of the empirical materials collected was inductive and iterative. The four techniques in qualitative data analysis, as outlined by Kaplan & Maxwell, consisting of: 1) coding, 2) analytical memos, 3) displays, and 4) contextual and narrative analysis and the six step data analysis and representation for case studies, as suggested by Creswell, were incorporated in the study. (Creswell, 2013; Kaplan & Maxwell, 1994) The six steps include: 1) data organization, 2) reading and memoing, 3) describing the data into codes and themes, 4) classifying the data into codes and themes; 5) interpreting the data, and 6) representing and visualizing the data. (Creswell, 2013)

Within Case Analysis:

Summative evaluations containing a detailed description of each case based on empirical material gathered from the interviews, observations, and documents secured were constructed. In addition, visual representations such as tables were provided to highlight themes or issues within the four cases.

Cross Case Analysis:

A number of comparisons of the four cases containing parts of the summative evaluations describing the key issues or themes were created to uncover any differences or commonalities.

Validity Strategies

Validity strategies were necessary due to the fact that qualitative research is basically subjective in nature as opposed to the objective nature of quantitative research. Kaplan and Maxwell state, “Due to the researcher’s proximity to the situation and the process being studied, they are more likely to catch important empirical material that may have been missed by a more objective form of research”. (Kaplan & Maxwell, 1994) The validity strategies selected for the study are: 1) rich data, 2) triangulation, and 3) feedback or member checking. (Creswell, 2012; Kaplan & Maxwell, 1994) Rich data entails the level of detail of the data collected so that very little information may be missed by the researcher. Triangulation helps support validity by utilizing many different sources of data such as open ended interviews, existing documentation, and observation to be able to substantiate the resulting data analysis. Another example of triangulation in the research study is the analysis of multiple cases which can also provide substantiation to the resulting data analysis. Feedback or member checking allows the subjects to review the information that the researcher has recorded to ascertain that the information is not only recorded correctly but within the essence or spirit of the information conveyed. (Creswell, 2012; Kaplan & Maxwell, 1994)

CHAPTER 4

FINDINGS

The findings of the case study research are presented in two sections. The first section contains the within case analyses for each of the four cases. Each case is described in a summative evaluation. The second section contains the cross case analyses.

Within Case Analysis

Summative evaluations containing a detailed description of each case based on the empirical material gathered from interviews, observations, and documentation are presented.

Case One:

Background: The small medical clinic in case one is a general family practice having a single physician age 55, one office staff member and one nursing staff member. While the physician has practiced medicine for many years in another area, the practice information used in the case study has been in business at this location for six months. It is located within a multi-unit single story building on a major state highway in a commercial area. There is an alarm system to protect the medical practice.

General Overview: The physician is technically oriented and has experienced a variety of situations involving EHR and HIPAA Compliance including: personally handling the IT related issues as a small healthcare provider, as a physician in a large franchised medical provider organization, and contracting with third party information systems services providers. Presently

to handle the rigors of IT security and compliance to HIPAA, the physician has joined a large local comprehensive health system management provider which is an integrated healthcare organization. The organization handles the electronic protected health records for the clinic and all of the information technology security and compliance issues and documentation related to ePHI for the practice. The practice uses the integrated healthcare organization's provided EPIC EHR and practice management software which is a fully integrated software solution for both hospital and clinic physicians.

Management Issues:

In response to, "Do you view the mandated compliance to the HIPAA Security Rule as an opportunity (or positive) to your practice or as a threat (or negative) to your practice and why?" Physician's view to this question was more in the middle as to whether the compliance issue was an opportunity or a threat. "Somewhere in-between the two." Physician would prefer a more defined choice or selection in answering the question.

In responding to, "Regarding the mandated compliance to the HIPAA Security Rule, do you feel that you have control in this situation or that you have no control in this situation and why?" Felt in control. This was due to the fact that the physician was very happy to have the option to have a comprehensive information system management services provider to completely handle his office needs on the issue.

On a scale of 1 to 5 with 1 feeling very high and 5 feeling very low, how would you rate your confidence in your current compliance situation if HHS showed up to perform an audit of your

practice today and why? A rating of "1" was given. Due to the large local comprehensive health system management provider's handling of the situation.

On a scale of 1 to 5 with 1 feeling very fearful and 5 feeling very unafraid, how would you rate your concern over an HHS audit of your practice resulting in non-compliance and why? The number "5" was the response. The same answer as above was given.

When questioned, "In general how does/has HIPAA compliance (Security Rule) impacted you and your practice?" Initially tried to accomplish the compliance for a time but it was too much work for the physician and his wife. The physician decided to join a large local comprehensive health system management solutions provider. Really likes the Epic software used by the solutions provider. Also, they handle all of the SOPs, security, documentation - everything.

When asked, "How do your feel about it? The government will pursue only if there is a specific agenda "to get you". You or your practice is a target for some reason. In the beginning did attend the seminars, workshops, and webinars presented by attorneys who preached a, "Comply or else!" situation. The physician did not think that the government would actually pursue individual practices without an agenda.

General compliance issues: Since the practice is a member of an integrated health organization, the organization handles all of the HIPAA Security Rule Standards, documentations, and all of the required activities which cover the information systems that create, amend, store, and transmit ePHI. Due to the arrangement with the integrated healthcare organization, the practice does have policies and procedures in place for physical security and information system security. The possible vulnerabilities and threats, and the resulting impact or risk to the practice has been

identified and the practice is protected against all reasonably anticipated threats or hazards to the security and integrity of ePHI. The integrated health organization has analyzed these problems and created a mitigation plan that it is working to decrease risks and vulnerabilities. The staff uses only desktop computers in the practice. The integrated health organization's technical staff handles the timely application of antivirus software and system patches to protect against malicious software and exploitation of vulnerabilities. It also monitors log-in attempts, has procedures for reporting and handling security incidents and has established a contingency plan that covers disaster recovery and back up. The integrated health organization provides the technical expertise to evaluate the information systems and uses a strategy and tool that considers all the elements of the HIPAA Security Rule, including all standards and implementation specifications. The organization handles the business associate contracts agreements and other arrangements that include security requirements to meet all the HIPAA Security Rule requirements per the HITECH Act. The organization has developed and implemented policies and procedures that address data back-up, data storage, and disposal of ePHI and / or the hardware and electronic media on which it is stored, including the appropriate methods to dispose of hardware, software and the data itself.

Specific technical security issues: The specific technical security issues of access controls, audit controls, integrity, person & entity authentication, and transmission security are managed by the integrated health organization along with the necessary documentation and business associate contract agreements in accordance with the HIPAA security rule standards.

Nursing/Office staff issues: The nursing and office staff members interviewed said that the practice does use unique passwords and that they are kept secret. There is an electronic

procedure that automatically terminates an electronic session after a predetermined time of inactivity. They have been trained on the security policies and procedures and they use only the practice's desktop computers.

Responses to the question, "How does/has the compliance mandate to HIPAA especially the Security Rule impact/ed you?" It does involve more paperwork. It is important to be careful and to follow the rules.

Responses to the question, "How do your feel about it?" One respondent said they did not mind having to follow the rules and one said that they feel it is a very difficult position/situation to be in. The table below is a snapshot of case one main issues.

Table 1. Case 1 Snapshot

Background	Medical practice; one physician; 2 nursing/office staff; 6 months at this location	
Overview	Joined large, local integrated healthcare organization. No EHR on site	
Management	Opportunity or Threat	In the middle
	Control or No Control	Control
	Confidence:1 very high/5 very low	1
	Fear of Non-compliance: 1 very fearful/5 very unafraid	5
	How practice impacted	Joined integrated organization for the services provided with HIPAA compliance.
	How feel about impact	Most individual practices should be okay if not a target.
Gen Compliance	Integrated healthcare organization handles all compliance issues, actions, and documentation.	
Specific Technical	Integrated healthcare organization handles all compliance issues,	

	actions, and documentation.
N/H/O staff	More paperwork. Must follow rules. /Don't mind. Very difficult.
Website	Due to membership, website offers patients considerable interaction/information
Documents	Integrated healthcare organization handles all compliance issues, actions, and documentation.
EHR software	EPIC EHR management software fully integrates hospitals and clinics.
IT services	Integrated healthcare organization's IT staff handles all network issues.

Case Two:

Background: The dental practice in case two is actually an orthodontic clinic. The practice has been in business for over twenty years. It consists of one orthodontist age 65 and a seven member staff of hygienists and office personnel. The practice exists as the only business in a single story building located within a mixed commercial/residential area. The building does have an alarm system.

General Overview: The practice does not have electronic protected health information resident on the practice's system. All electronic protected health information is entered directly into the Cloud9Ortho application software. The Cloud9Ortho is an orthodontic cloud and web based practice management software. The application service solution provides a secure EHR database along with system security compliance activities and documentation. The practice does have the required business associate contract agreement with the application provider detailing all services provided and the compliance mandate to HIPAA.

Management Issues:

When questioned whether the orthodontist viewed the mandated HIPAA Security Rule compliance as an opportunity or threat to the practice, the orthodontist definitely view it as a threat having negative impact.

When questioned whether the event of mandated compliance is viewed by the as orthodontist having control of the event (HIPAA Security Rule Compliance) or no control over the event, the response was that the orthodontist had no control over the mandated compliance. No chance to refuse to get involved. No choice. It was a major situation that had to be dealt with.

On a scale of 1 to 5 with 1 feeling very high and 5 feeling very low, how would you rate your confidence in your current compliance situation if HHS showed up to perform an audit of your practice today and why? A rating of 1 – 2 was given. This is due to the fact that all of the ePHI is handled and stored off site using Cloud 9 software. All protected patient information is handled in this manner. There is no protected patient information residing on the office system. The software provider handles all documentation needed for the HHS audit. The practice does have the appropriate written business associate contract agreements with the software provider.

On a scale of 1 to 5 with 1 feeling very fearful and 5 feeling very unafraid, how would you rate your concern over an HHS audit of your practice resulting in non-compliance and why? A rating of 4-5 was given. Being found non-compliant would be unpleasant, but it is highly unlikely given the use of the Cloud 9 software.

When questioned, “How has the HIPAA security rule compliance impacted the practice?” Initially prior to the approximately three inch document which outlined the suggested guidelines

and recommendations by the American Orthodontic Association for members, it was a very complex undertaking. However, the Association was very helpful in providing the information specifically tailored to the practice.

When asked, “How do you feel about HIPAA Compliance?” The orthodontist was very thankful that the association provided its members with the guidance and information necessary to accomplish the burdensome task of compliance.

General compliance issues: Since the Cloud9Ortho organization handles all of the HIPAA Security Rule requirements that cover the information systems involving EHR the orthodontist felt that these issues were not of his concern.

Specific technical security issues: These issues were handled by the Cloud 9 Ortho application organization. However, the practice does have the necessary documentation on the business associate contract agreements with Cloud 9 Ortho Company which specifically stipulates compliance with HIPAA security rule standards and requirements especially the technical standards covering access control, audit control, integrity, person & entity authentication, and transmission security.

Dental Hygienists/Office staff issues: The hygienists and office staff all stated that the organization did use unique passwords for each individual and that the passwords were kept private. The hygienists and office staff also said that their systems did automatically terminate after a predetermined time of inactivity, and that they had be trained on the clinic’s security policies and procedures covering electronic patient records having to with the “Cloud”.

When asked, “How does/has the compliance mandate to HIPAA especially the Security Rule impact/ed you?” The majority felt positive with comments: “With information going right into the Cloud, there is no shredding”; “More precise and detailed information”; “Very positive – while the workload has increased, we are getting the right information and more information – and more is better!”; “Must be very careful about the release of information.” However, there were others that did not feel any effect or difference.

When asked, “How do your feel about it?” The majority felt positive about the compliance. And while some said they loved it, other said that they did not feel any effect either way. The table below is a snapshot of case 2 main issues.

Table 2. Case 2 Snapshot

Background	Dental/orthodontic practice. One orthodontist; 7 hygienists/office staff; over 25 years at this location.	
Overview	Does not have EHR on office system. Uses a 3th party solutions provider	
Management	Opportunity or Threat	Threat
	Control or No Control	No Control
	Confidence:1 very high/5 very low	1-2
	Fear of Non-compliance: 1 very fearful/5 very unafraid	4-5
	How practice impacted	Changes had to be made. Very thankful to the AOA for guidance.
	How feel about impact	Very burdensome task
Gen Compliance	Relies on the cloud provider for compliance issues.	
Specific Technical	Relies on the cloud provider for compliance issues.	
N/H/O staff	Most very positive. Better patient information /Love it.	
Website	Offers practice information, contact info, and ability to schedule appointments. No individual patient health information provided.	

Documents	Does not have documentation relating to the Security Rule of HIPAA.
EHR software	Cloud9Ortho
IT services	Handles minimal tasks such as anti-virus protection. All practice management data/records are “in the cloud”.

Case Three:

Background: The dental practice is a single dentist office with a hygienist and office staff of six. The practice has been in business for twelve years. It is located in a single level building unit of a multi-unit complex of three buildings housing other small healthcare practices. The office complex is located within a mixed commercial/residential area. The dental practice does have an alarm system.

General Overview:

The office manager is the identified individual responsible for HIPAA compliance for the practice. The practice is handling the security compliance issues of the ePHI by themselves. They have invested the time, energy, and finances into creating and maintaining a security compliance plan. A few years ago accomplishing this task was very difficult for this small practice until the American Dental Association started to provide assistance to the dental industry through guidelines and documents which tailored the complex and comprehensive HIPAA compliance issues to focus and align with small dental practices. The guide is a step by step tool kit which contains flow charts and detailed information to help dental practices design and implement a compliance program. The tool kit contains all of the sample documentations necessary for compliance. The sample documents allow the user to follow the instructions and

insert the proper information. There is also guidance on the required training programs for the practice's staff necessary for compliance. The office manager is very dedicated to educating herself on all of the standards and related issues necessary for HIPAA compliance. The information provided by the ADA and other sources allow the office manager to work through the entire process of what needs to be accomplished and how to best accomplish the compliance issues in the "appropriate and reasonable" manner in alignment with the practice's level of risk to affect compliance. Everyone in the practice is well trained and dedicated to assuring HIPAA compliance and ensuring patient information security. While the practice does utilize a network services company on rare occasions, the office manager is performing all of the required network activities, security implementations, and audit tasks for the practice. Additionally, the Eaglesoft dental practice management software with Eaglesoft Clinician/EHR is used by the practice.

Management issues:

The dentist considers the HIPAA Security Rule compliance to be a threat to the practice. The functional aspect of compliance and the concern of not complying impact the practice in every aspect financial, clinical, emotional, even how the staff is affected. It is a very intrusive situation and causes an added dimension of concern and anxiety to be consistently diligent to adhering to the HIPAA rules. It affects every activity in the practice.

Regarding the mandated compliance, the dentist feels as though he has no control over the situation. They have absolutely no recourse but to comply.

On a scale of 1 to 5 with 1 feeling very high and 5 feeling very low, how would you rate your confidence in your current compliance situation if HHS showed up to perform an audit of your

practice today and why? A rating of "2" was given. Due to the efforts of the office manager and staff, the principal feels that they would score well in an audit. This is also due to the high amount of financial commitment along with the time and energy invested into the compliance efforts. The reason that a rating of 1 was not given is that HHS would probably find something negative to mention within the audit results.

On a scale of 1 to 5 with 1 feeling very fearful and 5 feeling very unafraid, how would you rate your concern over an HHS audit of your practice resulting in non-compliance and why? A rating of "1" was given. The principal is very fearful of an audit result of non-compliance. It could be very devastating personally (financial fines) and professionally (loss of reputation) depending on the reasons for the non-compliance.

When questioned, "In general how has/does/has HIPAA compliance (Security Rule) impacted you and your practice? It has impacted every aspect: financially, emotionally, clinically, and the staff. It has a financial impact on the practice and is very time consuming.

When asked, "How do your feel about it?" Very intrusive. Causes an added dimension of concern/anxiety to be constantly diligent to the demands placed by HIPAA compliance.

General compliance issues: The practice does have policies and procedures in place for physical security and information system security. The practice has identified possible vulnerabilities and threats, and the resulting impact or risk to your practice, has protected against all reasonably anticipated threats or hazards to the security and integrity of ePHI, and has analyzed these problems and created a mitigation plan that it is working to decrease risks and vulnerabilities. The practice does not use lap tops, PDAs, tablets, smart phones, or other similar tools within

their network. The office manager handles all network security activities such as the timely application of antivirus software and system patches to protect against malicious software and exploitation of vulnerabilities. The practice performs a number of auditing procedures including the monitoring of log-in attempts. Additionally the practice does have a procedure for reporting and handling security incidents. The practice has established a contingency plan that covers disaster recovery and back up. The practice uses the ADA HIPAA Compliance tool kit that considers all the elements of the HIPAA Security Rule, including all standards and implementation specifications. The business associate contracts and other agreements are included within the ADA HIPAA Compliance tool kit. The practice does monitor physical access to the information system to detect and respond to physical security incidents and have developed and implemented policies and procedures that address data back-up, data storage, and disposal of ePHI and / or the hardware and electronic media on which it is stored, including the appropriate methods to dispose of hardware, software and the data itself.

Specific technical security issues:

Access controls – The practice has identified all applications, systems, servers and other electronic tools that hold and use ePHI and has an access control procedures policy that includes rules of user behavior and consequences for failure to comply and has this policy been communicated to your system users. The practice has an electronic procedure that automatically terminates electronic session after a predetermined time of activity and a process or mechanism to encrypt and decrypt ePHI.

Audit Controls – The practice has determined the appropriate scope of audit controls that are be necessary to protect the information systems that contain ePHI based on our risk assessment. The practice did inventory its systems, applications, processes, servers, and other devices that make data vulnerable to unauthorized or inappropriate tampering, uses or disclosures of ePHI, has tools in place for auditing data review, creating, deleting and updating, plus for firewall system activity and other similar activities, and performs the audits necessary for compliance.

Integrity – The practice has a formally documented set of integrity requirements that is based on our analysis of use, users and misuses of ePHI and our risk analysis, has electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.

Person and Entity Authentication – The practice does have person and entity authentication policies and procedures and uses unique passwords for each member on specific systems within our system.

Transmission Security – The practice has implemented encryption for ePHI transmission.

Dental Hygienists/Office staff issues: Verified password management, log out sessions, advised/trained on security policies and procedures is in effect in practice.

How does/has the compliance mandate to HIPAA especially the security rule impact/ed you? Has made job much easier. Tasks are very defined and processes are followed consistently. Has not experienced a change.

How do you feel about it? It improves the accuracy of patient information (not having to read others' handwriting). It is easier to access patient information and you have documentation. Has not experienced a change. The table below is a snapshot of case three main issues.

Table 3. Case 3 Snapshot

Background	Dental practice; one dentist; hygienists/office staff of 6; practice 12 years.	
Overview	Office manager very active in all areas of compliance. EHR on site.	
Management	Opportunity or Threat	Threat
	Control or No Control	No Control
	Confidence:1 very high/5 very low	2
	Fear of Non-compliance: 1 very fearful/5 very unafraid	1
	How practice impacted	Every aspect: financially, emotionally, clinically, and the staff involvement.
	How feel about impact	Very intrusive. Causes concern/anxiety to be diligent.
Gen Compliance	Due to the ADA HIPAA Compliance ToolKit – have all general compliance issues covered.	
Specific Technical	Due to the ADA HIPAA Compliance ToolKit and other resources have all technical compliance issues covered.	
N/H/O staff	Has made job easier; very defined tasks & processes/ Improves accuracy.	
Website	Offers practice information, contact info, and ability to schedule appointments. No individual patient health information provided.	
Documents	Has all required documentation by using the toolkit's step by step/follow the diagram/fill in the boxes guidance materials.	
EHR software	Eaglesoft Clinician/EHR dental practice management software	
IT services	All IT services are performed by the office manager.	

Case Four:

Background: The medical practice in case four is a specialty practice. The practice has been established for over fifteen years ago and has been involved in EHR since 2004. The practice has a total of 14 members including the physicians, nursing staff, office staff, and an in-house lab attendant. It is located on the first floor of a two story building which is part of a multiple building medical complex. The complex is set in a secluded area well off a main US highway which is commercial. The medical practice does have an alarm system.

General Overview: The practice has selected the PrimeSUITE integrated electronic health record (EHR) and practice management solution from Greenway Health. Greenway's PrimeSUITE practice management application software handles the practice's work flow, scheduling, and the patient health information. While patient health information is resident and backed up within the clinic, Greenway does provide the backup files as off-site storage for disaster recovery in the clinics' contingency plan. Since the individual identified by the clinic as the person responsible for IT does not have extensive technical expertise needed to provide the system administration duties, the practice has contracted with a local company to provide all of the necessary HIPAA required information management system services including documentation. The practice does have the proper business associates contract agreements with both of companies mentioned.

Management Issues:

Do you view the mandated compliance to the HIPAA Security Rule as an opportunity (or positive) to your practice or as a threat (or negative) to your practice and why? An opportunity.

Encourages good business practices; consistency in protecting data and patient information. Encourages strong training and follow-up.

Regarding the mandated compliance to the HIPAA Security Rule, do you feel that you have control in this situation or that you have no control in this situation and why? Control. Regulations are clear, more established. Expectations are clear and staff trained to manage efficiently.

On a scale of 1 to 5 with 1 feeling very high and 5 feeling very low, how would you rate your confidence in your current compliance situation if HHS showed up to perform an audit of your practice today and why? A rating of 2 was given. We have established a more reliable IT system to aid in the management of compliance.

On a scale of 1 to 5 with 1 feeling very fearful and 5 feeling very unafraid, how would you rate your concern over an HHS audit of your practice resulting in non-compliance and why? A rating of 3 was given. Audits are always concerning but also help practices to correct and improve.

When questioned, “In general how does/has HIPAA compliance (Security Rule) impacted you and your practice?” Has sharpened our focus on running our practice on a higher plane of business management. We have had to strengthen our training and development to ensure that all levels of staff understand compliance.

When asked, “How do your feel about it?” We have had to make decisions that affect how we run the practice. It has cost us more in time and money and we have had to adjust how we do business. I feel as though we have done a good job working toward solid compliance, but it has

made our days more complicated and detailed. There is more pressure on a daily basis to meet the checks and balances of compliance.

General Compliance Issues: The practice does have policies and procedures in place for physical security and information system security. The practice utilizes a local network services company to provide the risk analysis and management activities for HIPAA compliance documentation. The network services company has identified the possible vulnerabilities and threats, and the resulting impact to the practice in accordance with the principals' input to level of risk. The network services company protects the practice against all reasonably anticipated threats or hazards to the security and integrity of ePHI and analyzes these problems to create a mitigation plan that it is working to decrease risks and vulnerabilities. The staff does not utilize components such as PDAs, tablets, or smart phones while in the office environment. However, the physicians do have remote access to the clinic's information system. The network services company handles the timely application of antivirus software and system patches to protect against malicious software and exploitation of vulnerabilities along with remotely monitoring log-in attempts. The practice does have a procedure for reporting and handling security incidents and the practice does have a contingency plan that covers disaster recovery and back up. Since the practice's staff does not have the technical experience to evaluate the systems, an experienced local network management services company is under contract to provide these services. The practice does have a strategy to consider all the elements of the HIPAA Security Rule, including all standards and implementation specifications. The practice does have business associate contracts agreements and arrangements which include security requirements to meet all of the HIPAA Security Rule requirements per the HITECH Act.

Specific Technical Issues: The practice has technical expertise under contract.

Access controls: The local network management services provider does have access to technical policies and procedures and they have identified all applications, systems, servers and other electronic tools that hold and use ePHI. The practice does have an electronic procedure that automatically terminates an electronic session after a predetermined time of inactivity and the practice does encrypt and decrypt ePHI. The practice does have an access control procedures policy that includes rules of user behavior and consequences for failure to comply and has this policy been communicated to your system users.

Audit Controls: The local network management services provider provides all audit services, performance services, and monitoring services as needed for compliance remotely on a periodic basis.

Integrity: The person with the responsibility for IT said that she was unsure of specific integrity policies and procedures but that the local network management services provider did provide the services/mechanisms for preventing data from being altered or destroyed in an unauthorized manner and authentication mechanisms. The practice believes that the local network management services provider does provide a high level of assurance that information integrity is being maintained.

Person and Entity Authentication: The practice does have authentication policies and procedures. The practice utilizes unique passwords that are kept private and secret. The practice does use a third party for authentication /network support.

Transmission Security: The practice has implemented encryption for ePHI transmission.

Nursing & Office Staff Issues: The nursing and office staff that was interviewed said that the practice does use passwords. They are unique for each individual and are not shared. The practice does have an electronic procedure that automatically terminates an electronic session after a predetermined time of inactivity. The nursing and office staff that was interviewed reported that they have been trained on the clinic's security policies and procedures covering electronic patient records and that they have had retraining/refreshing/reminding periodically. The office and nursing staff do not use components such as a lap top, PDA, tablet, smart phone, and/or other similar tools. They only use the desktop or the examining room computer equipment.

Responses to the question, "How does/has the compliance mandate to HIPAA especially the Security Rule impact/ed you?" Being constantly diligent and careful to follow the rules and that the rules are followed by everyone. The automation of procedures has made some aspects of the job easier.

Responses to the question, "How do your feel about it?" It is additional stress and it is expensive for the practice. It is helpful. The table below is a snapshot of case 4 main issues.

Table 4. Case 4 Snapshot

Background	Medical specialty practice; 2 physicians, 12 member staff; in practice over fifteen years.	
Overview	EHR on site. Uses a practice management/ EHR application software and local network services/management provider.	
Management	Opportunity or Threat	Opportunity
	Control or /No Control	Control
	Confidence:1 very high/5 very low	2
	Fear of Non-compliance: 1	3

	very fearful/5 very unafraid	
	How practice impacted	Has sharpened focus; strengthen staff training and development.
	How feel about impact	Costs more in time and money; had to adjust how we do business.
Gen Compliance	Compliance issues/actions/documentation provided by local network services/management provider.	
Specific Technical	Compliance issues/actions/documentation provided by local network services/management provider.	
N/H/O staff	Constantly diligent to follow rules; makes job easier/ added stress; expensive.	
Website	Offers practice information, contact info, and ability to schedule appointments. No individual patient health information provided.	
Documents	All compliance documentation provided by local network services/management provider.	
EHR software	Greenway PrimeSuite integrated EHR and practice management software.	
IT services	Local network services/management provider.	

Cross Case Analysis

The cross case analyses consist of four cases: two are small medical practices and two are small dental practices.

Background Characteristics

The medical practices represent a single physician family practice labeled case 1 and the other is a two physician specialty practice labeled case 4. The dental practices include a single dentist family practice labeled case 3 and a single orthodontic practice labeled case 2. The focus of the case study was compliance to the HIPAA Security Rule and information system security with related issues. The table below compares the four cases on background characteristics.

Table 5. Background Characteristics

Background	Case 1	Case 2	Case 3	Case 4
Type	family medical	orthodontic	general dentistry	medical specialty
# of principals	one physician	one orthodontist	one dentist	two physicians
Approximate age of principals	55	65	45	48 / 48
Size of staff	two	eight	six	twelve
Years in practice at current location	6 months (at this location)	over 25 years	12 years	over 15 years

EHR and IT Issues

Each practice handled the compliance issue differently. In case 1 the practice joined a large local integrated healthcare organization that handles all of the HIPAA Security Rule compliance issues and the practice's information system security. In case 2 the practice contracted with a third party software application as a service provider where all electronic patient health information resides within the cloud. With this arrangement the HIPAA Security Rule compliance and related information system security issues are the responsibility of the software application as a service provider as stated in the business associate contract agreement with the practice. In case 3 the practice has taken full responsibility for the HIPAA Security Rule compliance and the related information system security issues. Finally, in case 4 the practice has taken responsibility for the HIPAA Security Rule compliance and the related

information system security issues, but has contracted with a local network services management company to provide all activities and documentation necessary for compliance. The practice has the business associate contract agreement necessary for compliance. The table below compares the four cases on EHR issues.

Table 6. EHR and IT Issues

EHR issues	Case 1	Case 2	Case 3	Case 4
EHR on site	No	No	Yes	Yes
EHR software	EPIC	Cloud9Ortho	Eaglesoft	Greenway PrimeSUITE
EHR solutions	Integrated healthcare org provided	3rd party cloud provider	Uses practice mgmt/ehr software	Uses practice mgmt/ehr software
IT services	Integrated healthcare org provided	Office staff handles minimal tasks	In house IT services accomplished	Contracted with local network services/ management company

Management Issues

The management issues analyzed in the case study involved a number of topics covering: 1) whether the principals viewed the mandated HIPAA Security Rule compliance was an opportunity or a threat; 2) whether the principals felt that they had control or no control over the mandated HIPAA Security Rule compliance; 3) how confident they felt about an HHS audit of the practice; 4) how they felt about the "fear of non-compliance" concept; 5) how HIPAA Security Rule compliance impacted their practice; and 6) how they felt about the impact. The following table shows the responses by each case to the management issues raised concerning the HIPAA Security Rule compliance. See the following table below.

Table 7. Management Issues

Management issues	Case 1	Case 2	Case 3	Case 4
Opportunity or Threat	In the middle	Threat	Threat	Opportunity
Control or No Control	Control	No Control	No Control	Control
Confidence on an HHS audit outcome where: 1 very high/5 very low	1	1-2	2	2
Fear of Non-Compliance where: 1 very fearful/5 very unafraid	5	4-5	1	3
Impact on practice	Joined integrated healthcare organization for the services provided	Changes had to be made.	Every aspect of practice: financially, emotionally, clinically, staff involvement	Has sharpened focus; strengthen staff training and development
Feelings on Impact on practice	Okay	Very burdensome task	Very intrusive. Causes concern and anxiety to be diligent	Costs more in time and money. Had to adjust how we do business

Compliance Issues

The case study analyzed the general compliance issues and the specific technical issues involved in HIPAA Security Rule compliance. The table below provides information on the four

cases' view on the practices' general compliance issues and the specific technical issues covered in HIPAA Security Rule compliance.

Table 8. Compliance Issues

Compliance Issues	Case 1	Case 2	Case 3	Case 4
General	Membership in the integrated healthcare organization provides all of the compliance issues, actions, and documentation.	Relies on the cloud provider to cover the compliance issues.	Due to the ADA HIPAA Compliance Toolkit the practice states that it has all of the general issues covered.	Compliance issues/actions/documentation are provided by the practice management/EHR software and the local network services management provider.
Specific technical	Membership in the integrated healthcare organization provides all of the compliance issues, actions, and documentation.	Relies on the cloud provider to cover the compliance issues.	Due to the ADA HIPAA Compliance Toolkit and other resources the practice states that it has all of the specific technical issues covered.	Compliance issues/actions/documentation are provided by the practice management/EHR software and the local network services management provider.

Impact on Practice/Task and Feelings on Compliance Impact Issues

Two questions were posed to the physicians and dentists and their staff asking how HIPAA compliance impacted them and how they felt about it. The physicians and dentists answered on the impact to them and their practice while the staff reported on the impact regarding their tasks. The first table below provides information on the four cases' views on

HIPAA compliance impact by the physicians and dentists and their staff on the practice/tasks. The second table below provides information on the four cases' views on HIPAA compliance impact and how they felt about it.

Table 9. Impact on Practice/Task Issues

	Category	In general, how does/has HIPAA compliance (Security Rule) impacted you [and your practice]?
Case 1	Physician	Initially tried to accomplish the compliance for a time but it was too much work for the physician and his wife. The physician decided to become a member of a large local integrated organization. Really likes the Epic software used by the solutions provider. Also, they handle all of the SOPs, security, documentation - everything.
	Staff	It does involve more paperwork. It is important to be careful and to follow the rules.
Case 2	Dentist	Initially prior to the approximately three inch document which outlined the suggested guidelines and recommendations by the American Orthodontic Association for members, it was a very complex undertaking. However, the Association was very helpful in providing the information specifically tailored to the practice.
	Staff	The majority felt positive with comments: "With information going right into the Cloud, there is no shredding"; "More precise and detailed information"; "Very positive – while the workload has increased, we are getting the right information and more information – and more is better!"; "Must be very careful about the release of information." However, there were others that did not feel any effect or difference.
Case 3	Dentist	It has impacted every aspect: financially, emotionally, clinically, and the staff. It has a financial impact on the practice and is very time consuming.
	Staff	Has made job much easier. Tasks are very defined and processes are followed consistently. Has not experienced a change.
Case 4	Physician	Has sharpened our focus on running our practice on a higher plane of business management. We have had to strengthen our training and development to ensure that all levels of staff understand compliance.
	Staff	Being constantly diligent and careful to follow the rules and that the rules are followed by everyone. The automation of procedures has made some aspects of the job easier.

Table 10. Feelings on Compliance Impact Issues

	Category	How do your feel about it [HIPAA compliance]?
Case 1	Physician	The government will pursue only if there is a specific agenda "to get you". You or your practice is a target for some reason. In the beginning did attend the seminars, workshops, and webinars presented by attorneys who preached a, "Comply or else!" situation. The physician did not think that the government would actually pursue individual practices without an agenda.
	Staff	One respondent said they did not mind having to follow the rules and one said that they feel it is a very difficult position/situation to be in.
Case 2	Dentist	The orthodontist was very thankful that the association provided its members with the guidance and information necessary to accomplish the burdensome task of compliance.
	Staff	The majority felt positive about the compliance. And while some said they loved it, other said that they did not feel any effect either way.
Case 3	Dentist	Very intrusive. Causes an added dimension of concern/anxiety to be constantly diligent to the demands placed by HIPAA compliance.
	Staff	It improves the accuracy of patient information (not having to read others' handwriting). It is easier to access patient information and you have documentation. Others responded that they have not experienced a change.
Case 4	Physician	We have had to make decisions that affect how we run the practice. It has cost us more in time and money and we have had to adjust how we do business. I feel as though we have done a good job working toward solid compliance, but it has made our days more complicated and detailed. There is more pressure on a daily basis to meet the checks and balances of compliance.
	Staff	It is additional stress and it is expensive for the practice. It is helpful.

CHAPTER 5

SUMMARY AND CONCLUSIONS

Research Questions Analysis

In analyzing the research questions for the case study, each question is addressed; however, the six sub-questions will be covered first. The central question is considered at the end. The sub-questions, each case situation, and conclusion by the researcher are provided below.

Sub-Question 1 – How do the medical and dental practices assess the security of their information systems regarding identifying possible vulnerabilities?

Case 1 – Considered options available and decided to partner with a large and comprehensive health organization that actively maintains all member entities' systems in compliance with the HIPAA Security Rule.

Case 2 – utilizes a cloud based solution to provide the EHR security compliance issues.

Case 3 – diligently following a carefully constructed security plan based on the guidance framework provided by the American Dental Association to analyze and to monitor the practice's system for vulnerabilities through a variety of auditing activities.

Case 4 – uses a local network services management company to provide the required information system network activities regarding vulnerability identification and the resulting documentation for HIPAA compliance.

Researcher – Each practice in the case study has chosen a different approach to handling the need to assess system vulnerabilities. Three of the four have concluded that it is best for the

practice to enter into an agreement with a knowledgeable third party to accomplish the goal of assessing security by identifying possible system vulnerabilities. Only one practice has decided to undertake the assessment of the security of their information system regarding identifying possible vulnerabilities by performing the various tasks and activities necessary to ensure that vulnerability identification and the actions necessary to prevent or mitigate the known vulnerability is performed and monitored. See table below for responses.

Table 11. Sub Question #1

Sub Q #1	How do the medical and dental practices assess the security of their information systems regarding identifying possible vulnerabilities?
Case 1	Considered options available and decided to partner with a large and comprehensive health organization that actively maintains all member entities' systems in compliance with the HIPAA Security Rule.
Case 2	Utilizes a cloud based solution to provide the EHR security compliance issues.
Case 3	Diligently following a carefully constructed security plan based on the guidance framework provided by the American Dental Association to analyze and to monitor the practice's system for vulnerabilities through a variety of auditing activities.
Case 4	Uses a local network services management company to provide the required information system network activities regarding vulnerability identification and the resulting documentation for HIPAA compliance.
Researcher	Each practice in the case study has chosen a different approach to handling the need to assess system vulnerability. Three of the four have concluded that it is best for the practice to enter into an agreement with a knowledgeable third party to accomplish the goal of assessing security by identifying possible system vulnerabilities. However, each of the three has chosen a different strategy in the utilization of the service providing entity. Only one practice has decided to undertake the assessment of the security of their information system regarding identifying possible vulnerabilities by performing the various tasks and activities necessary to ensure that vulnerability identification and the actions necessary to prevent or mitigate the known vulnerability is performed and monitored.

Sub-Question 2 – How are security practices and internal system controls implemented?

Case 1 – a large integrated health organization's technology team actively maintains the practice's information system for compliance with the HIPAA Security Rule.

Case 2 – has a business associates contract agreement with the cloud based solutions provider stipulating that the provider follows the security practices and implements the necessary internal system controls for compliance with the HIPAA Security Rule.

Case 3 – follows a very comprehensive and thorough process to ensure that the necessary security practices and internal controls are selected, consistently applied and monitored.

Case 4 – relies on a local network system services management company to provide the necessary security procedures to the practice and to ensure that the proper internal controls are selected, applied and monitored. The practice has business associates contract agreements with both the local network system services management company and the EHR/practice management solutions provider stipulating that the organizations follows the security practices and implements the necessary internal system controls for compliance with the HIPAA Security Rule.

Researcher - Again each practice in the case study has chosen a different approach to handling the need for implementing security practices and having the proper internal system controls. Three of the four have concluded that it is best for the practice to enter into an agreement/membership with a knowledgeable third party to accomplish the goal of implementing security practices and the proper internal system controls. Only one practice has

decided to undertake the selection and implementation of the security practices and the actions of applying the necessary internal controls to secure their system. See table below for responses.

Table 12. Sub Question #2

Sub Q#2	How are security practices and internal system controls implemented?
Case 1	A large local integrated health organization's technology team actively maintains the practice's information system for compliance with the HIPAA Security Rule.
Case 2	Has a business associates contract agreement with the cloud based solutions provider stipulating that the provider follows the security practices and implements the necessary internal system controls for compliance with the HIPAA Security Rule.
Case 3	Follows a very comprehensive and thorough process to ensure that the necessary security practices and internal controls are selected, consistently applied and monitored.
Case 4	Relies on a local network system services management company to provide the necessary security procedures to the practice and to ensure that the proper internal controls are selected, applied and monitored. The practice has Business Associates Contract Agreements with both the local network system services management company and the EHR/practice management solutions provider stipulating that the organizations
Researcher	Again each practice in the case study has chosen a different approach to handling the need for implementing security practices and having the proper internal system controls. Three of the four have concluded that it is best for the practice to enter into an agreement with a knowledgeable third party to accomplish the goal of implementing security practices and the proper internal system controls. Only one practice has decided to undertake the selection and implementation of the security practices and the actions of applying the necessary internal controls to secure their system.

Sub-Question 3 – How confident are the physicians and dentists regarding their "perceived" compliance with the HIPAA Security Rule?

Case 1 – A rating of 1. Very confident due to the integrated healthcare organization's handling of every aspect of the HIPAA Security Rule compliance issues for the practice.

Case 2 – A rating of 1 – 2. Feeling good/confident in being found in compliance by an HHS audit. This is due to the fact that all of the ePHI is handled and stored off site using Cloud 9 software.

Case 3 – A rating of 2. Very confident due to the expenditures in equipment, technologies, and methodologies to secure system along with policies, procedures, and practices in use to assure compliance. The reason that a rating of 1 was not given is that HHS would probably find something negative to mention within the audit results.

Case 4 – A rating of 2. We have established a more reliable IT system to aid in management of compliance.

Researcher - All of the physicians and dentists of the case study practices are confident to very confident in their compliance with the HIPAA Security Rule. All feel that the steps that they have chosen for attaining compliance are successfully accomplishing that goal.

See table below for responses.

Table 13.Sub Question #3

Sub Q#3	How confident are the physicians and dentists regarding their "perceived" compliance with the HIPAA Security Rule?
Case 1	A rating of 1. Very confident due to the integrated healthcare organization's handling of every aspect of the HIPAA Security Rule compliance issues for the practice.
Case 2	A rating of 1 – 2. Feeling good/confident in being found in compliance by an HHS audit. This is due to the fact that all of the EHR is handled and stored off site using Cloud 9 software.
Case 3	A rating of 2. Very confident due to the expenditures in equipment, technologies, and methodologies to secure system along with policies, procedures, and practices in use to assure compliance. The reason that a rating of 1 was not given is that HHS would probably find something negative to mention within the audit results.
Case 4	A rating of 2. We have established a more reliable IT system to aid in the management of compliance.

Researcher	All of the physicians and dentists of the case study practices are confident to very confident in their compliance with the HIPAA Security Rule. All feel that the steps that they have chosen for attaining compliance are successfully accomplishing that goal.

Sub-Question 4 – How do the physicians' and dentists' fear of non-compliance influence security compliance?

Case 1 – Does not have a fear of non-compliance due to the decision to join the large integrated healthcare organization. However, does feel that the auditing process of the government is selective.

Case 2 – While an audit determination of being non-compliant would be unpleasant, it is highly unlikely given the use of the Cloud 9 Ortho software recommended by the Orthodontic Association.

Case 3 – Since the principal is very fearful of an auditing result of non-compliance, the compliance approach is well orchestrated and well funded.

Case 4 – Audits always concerning but also help practices to correct and improve.

Researcher – The physicians and one of the dentists report that they are not fearful or not as fearful of being found in non-compliance; whereas, one of the dentists felt very fearful of non-compliance. The dentist who expressed fearfulness decided to completely handle the compliance issue in house, while those who commented that they were not fearful or as fearful elected to have third party providers assist them in compliance. While a statement cannot be made as to how the fear of non-compliance has contributed to the selection made for security compliance, it should be noted that the most fearful is the most involved in the security and compliance effort. See table below for responses.

Table 14.Sub Question #4

Sub Q#4	How does the physicians' and dentists' fear of non-compliance influence security compliance?
Case 1	Does not have a fear of non-compliance due to the decision to join the large integrated healthcare organization. However, does feel that the auditing process of the government is selective.
Case 2	While an audit determination of being non-compliant would be unpleasant, it is highly unlikely given the use of the Cloud 9 Ortho software recommended by the Orthodontic Association.
Case 3	Since the principal is very fearful of an auditing result of non-compliance, the compliance approach is well orchestrated and well funded.
Case 4	Audits always concerning but also help practices to correct and improve.
Researcher	The physicians and one of the dentists report that they are not fearful or not as fearful of being found in non-compliance; whereas, one of the dentists felt very fearful of non-compliance. The dentist who expressed fearfulness decided to completely handle the compliance issue in house, while those who commented that they were not fearful or as fearful elected to have 3rd party providers assist them in compliance. While a statement cannot be made as to how the fear of non-compliance has contributed to the selection made for security compliance, it should be noted that the most fearful is the most involved in the security and compliance effort.

Sub-Question 5 – How do the physicians' and dentists' primary and secondary appraisals to compelled compliance influence security compliance?

Case 1 – Does not consider it an opportunity or a threat and based on the options available and feels there is situational control.

Case 2 –Definitely views it as a threat having negative impact to the practice and the principal felt that they had no control over the mandated compliance. No chance to refuse to get involved. No choice.

Case 3- The principal's primary appraisal is threat and the secondary appraisal is no control.

Case 4 – Considers it an opportunity. Encourages good business practices; consistency in protecting data and patient information. Encourages strong training and follow-up. Felt in control of the situation since the regulations are established and clear.

Researcher – While the two dentists felt that HIPAA compliance is a threat to their practice and that they are not in control of the situation, the two physicians felt HIPAA compliance is either an opportunity or neither an opportunity or a threat to their practice and that they have control of the situation. According to the article, "Understanding User Responses to Information Technology: A Coping Model of User Adaptation", by Anne Beaudry and Alain Pinsonneault, since the two dentists felt that the mandated compliance was a threat to their practice and that they felt that they had no control over the situation indicates that they would use the self-preservation coping method where the adaption efforts would be avoidance or non-existent. One of the physicians felt that the mandated compliance was an opportunity and felt that they did have control over the situation. According to Beaudry and Pinsonneault this indicates that the physician would use the benefits maximizing strategy where the adaptation efforts by the user will be broad and far reaching. Since one of the physicians felt in control of the situation but felt "in the middle" regarding issue of opportunity or threat, the physician could use either the benefits maximizing strategy or the disturbance handling strategy where the adaptation efforts are self-satisfying. The two physicians' responses seem to align with Beaudry's and Pinsonneault's coping method identification especially when paired with their responses to how they felt about the HIPAA compliance mandate. However, the two dentists' responses would indicate that their adaptation efforts would be avoidance or non-existent which is not the case since each has actively taken steps to comply with the mandate. Therefore, one could make the

statement that while the dentists' felt that they did not have control over choosing to comply, they did have control over how to comply. This would indicate that the dentists could use the disturbance handling strategy where the adaptation efforts are self-satisfying, which seem to better align with the actual situation and the results of Beaudry's and Pinsonneault's research.

In considering the article, "The Other Side of Acceptance: Studying the Direct and Indirect Effects of Emotions on Information Technology Use", also by Anne Beaudry and Alain Pinsonneault, the two dentists that felt that the mandated compliance was a threat to their practice and that they felt that they had no control over the situation indicates that they would place in the Loss Emotions quadrant of the Framework for Classifying Emotions. The emotions listed in the Loss Emotions quadrant are anger, dissatisfaction, disappointment, annoyance, frustration and disgust. The physician that felt that the mandated compliance was an opportunity and felt that they did have control over the situation would place in the Challenge Emotions quadrant. The emotions listed in the Challenge Emotions quadrant are excitement, hope, anticipation, arousal, playfulness, and flow. Finally the physician that felt in control of the situation but felt "in the middle" regarding issue of opportunity or threat would place in either the Challenge Emotions quadrant or the Deterrence Emotions quadrant. The emotions listed in the Deterrence Emotions quadrant are anxiety, fear, worry, and distress. Given this physician's comments that he was not worried about non-compliance and that he really liked the software offered by his membership with the large integrated healthcare organization, it seems as his emotions align more with the Challenge Emotions quadrant rather than the Deterrence Emotions quadrant. The other physician's emotions seem to align with the Challenge Emotions quadrant also given her comments that "[mandated compliance] has sharpened our focus on running our

practice on a higher plane of business management. One of the dentists does seem to place in the Loss Emotions quadrant given his response that [HIPAA compliance] was a burdensome task. Also, the other dentist does seem to be placed in the Loss Emotions quadrant given his response that [HIPAA compliance] is very intrusive. However, he could also fit into the Deterrence Emotions quadrant given his response that [HIPAA compliance] causes an added dimension of concern/anxiety. It appears that when the researcher considered all of the responses given by the physicians and dentists as opposed to just their primary and secondary appraisals of opportunity/threat and control/no control responses, the case study research does seem to be consistent with the findings of Beaudry and Pinsonneault. See table below for responses.

Table 15. Sub Question #5

Sub Q#5	How do the physicians' and dentists' primary and secondary appraisals to compelled compliance influence security compliance?
Case 1	Does not consider it an opportunity or a threat and based on the options available feels there is situational control.
Case 2	Definitely views it as a threat having negative impact to the practice and the principal felt that had no control over the mandated compliance. No chance to refuse to get involved. No choice.
Case 3	The principal's primary appraisal is threat and the secondary appraisal is no control.
Case 4	Considers it an opportunity. Encourages good business practices; consistency in protecting data and patient information. Encourages strong training and follow-up. Felt in control of the situation since the regulations are established and clear.
Researcher	Researcher – While the two dentists felt that HIPAA compliance is a threat to their practice and that they are not in control of the situation, the two physicians felt HIPAA compliance is either an opportunity or neither an opportunity or a threat to their practice and that they have control of the situation. According to the article, "Understanding User Responses to Information Technology: A Coping Model of User Adaptation", by Anne Beaudry and Alain Pinsonneault, since the two dentists felt that the mandated compliance was a threat to their practice and that they felt that they had no control over the situation indicates that they would use the self-preservation coping method where the adaption efforts would be avoidance or non-existent. One of the physicians felt that the mandated

	compliance was an opportunity and felt that they did have control over the situation. According to Beaudry and Pinsonneault this indicates that the physician would use the benefits maximizing strategy where the adaptation efforts by the user will be broad and far reaching. Since one of the physicians felt in control of the situation but felt "in the middle" regarding issue of opportunity or threat, the physician could use either the benefits maximizing strategy or the disturbance handling strategy where the adaptation efforts are self-satisfying. The two physicians' responses seem to align with Beaudry's and Pinsonneault's coping method identification especially when paired with their responses to how they felt about the HIPAA compliance mandate. However, the two dentists' responses would indicate that their adaptation efforts would be avoidance or non-existent which is not the case since each has actively taken steps to comply with the mandate. Therefore, one could make the statement that while the dentists' felt that they did not have control over choosing to comply, they did have control over how to comply. This would indicate that the dentists could use the disturbance handling strategy where the adaptation efforts are self-satisfying, which seem to better align with the actual situation and the results of Beaudry's and Pinsonneault's research. In considering the article, "The Other Side of Acceptance: Studying the Direct and Indirect Effects of Emotions on Information Technology Use", also by Anne Beaudry and Alain Pinsonneault, the two dentists that felt that the mandated compliance was a threat to their practice and that they felt that they had no control over the situation indicates that they would place in the Loss Emotions quadrant of the Framework for Classifying Emotions. The emotions listed in the Loss Emotions quadrant are anger, dissatisfaction, disappointment, annoyance, frustration and disgust. The physician that felt that the mandated compliance was an opportunity and felt that they did have control over the situation would place in the Challenge Emotions quadrant. The emotions listed in the Challenge Emotions quadrant are excitement, hope, anticipation, arousal, playfulness, and flow. Finally the physician that felt in control of the situation but felt "in the middle" regarding issue of opportunity or threat would place in either the Challenge Emotions quadrant or the Deterrence Emotions quadrant. The emotions listed in the Deterrence Emotions quadrant are anxiety, fear, worry, and distress. Given this physician's comments that he was not worried about non-compliance and that he really liked the software offered by his membership with the large integrated healthcare organization, it seems as his emotions align more with the Challenge Emotions quadrant rather than the Deterrence Emotions quadrant. The other physician's emotions seem to align with the Challenge Emotions quadrant also given her comments that "[mandated compliance] has sharpened our focus on

	running our practice on a higher plane of business management. One of the dentists does seem to place in the Loss Emotions quadrant given his response that [HIPAA compliance] was a burdensome task. Also, the other dentist does seem to be placed in the Loss Emotions quadrant given his response that [HIPAA compliance] is very intrusive. However, he could also fit into the Deterrence Emotions quadrant given his response that [HIPAA compliance] causes an added dimension of concern/anxiety. It appears that when the researcher considered all of the responses given by the physicians and dentists as opposed to just their primary and secondary appraisals of opportunity/threat and control/no control responses, the case study does seem to be consistent with the findings of Beaudry and Pinsonneault.

Sub-Question 6 – How do security compliance decisions differ in medical and dental practices?

Case 1 – chose to join a large integrated healthcare organization.

Case 2 – chose to follow the Orthodontic Association's recommendation in using the Cloud 9 Ortho software solution.

Case 3 – chose to follow the guideline framework provided by the American Dental Association and to purchase an EHR/practice management software solution and to have the practice handle the task of compliance by themselves.

Case 4 – chose to purchase an EHR/practice management software solution and chose to contract with a local network services management company handle the task of compliance.

Researcher - Each of the four practices chose a different security compliance strategy. The physician in case 1 had experienced a variety of security compliance situations in the past and at this point decided to partner with an organization that would handle every aspect of security compliance for the practice. The orthodontist in case 2 decided to follow the association's recommendation on using a cloud solution where the EHR would not reside on the practice's system. The dentist in case 3 decided to use the guidance framework provided by the dental

association and work through the compliance issues in house. The physicians in case 4 decided to handle the compliance mandate by utilizing third party solutions to deal with the compliance issues. While all four practices found workable solutions for their practice, only one chose the more involved "hands on" approach. There are not just differences between the medical and dental practices' decisions, but there are differences in the two medical practices' decisions and the two dental practices' decisions. There could be many possible reasons for the particular choices: age, more control, technically oriented staffer, and less contractual financial resources committed as in lower fixed cost to the practice among others. See table below for responses.

Table 16. Sub Question #6

Sub Q#6	How do security compliance decisions differ in medical and dental practices?
Case 1	Chose to join a large integrated healthcare organization.
Case 2	Chose to follow the Orthodontic Association's recommendation in using the Cloud 9 Ortho software solution.
Case 3	Chose to follow the guideline framework provided by the American Dental Association and to purchase an EHR/practice management software solution and to have the practice handle the task of compliance by themselves.
Case 4	Chose to purchase an EHR/practice management software solution and contract with a local network services management company to handle the task of compliance.
Researcher	Each of the four practices chose a different security compliance strategy. The physician in case 1 had experienced a variety of security compliance situations in the past and at this point decided to partner with an organization that would handle every aspect of security compliance for the practice. The orthodontist in case 2 decided to follow the association's recommendation on using a cloud solution where the EHR would not reside on the practice's system. The dentist in case 3 decided to use the guidance framework provided by the dental association and work through the compliance issues by themselves. The physicians in case 4 decided to handle the compliance mandate by utilizing third party solutions to deal with the compliance issues. While all four practices found workable solutions for their practice, only one chose the more involved "hands on" approach. There are not just differences between medical and dental practices' decisions, but there are differences in the

	two medical practices' decision and the two dental practices' decisions. There could be many possible reasons for the particular choices: age, more control, technically oriented staffer, and less contractual financial resources committed as in lower fixed cost to the practice among others.

The Central Question:

How compliant to the Security Rule of HIPAA and secure are information systems in the small medical and dental practices?

Based on the information gathered from the cases in the study, the medical and dental practices are diligent in identifying "reasonable and appropriate" measures in following the compliance issues of the Security Rule of HIPAA. The medical practice in case 1 has joined an integrated healthcare organization that provides the security policies, practices, mechanisms, and documentation for the practice to be in compliance. The dental practice in case 2 utilized an EHR cloud based solution where none of the patient's health records are resident at the practice and the solution provider is handling the compliance mandates to be in compliance. The dental practice in case 3 is engaged in every aspect of compliance by consistently following a guidance framework toolkit provided by the American Dental Association to be in compliance. The medical practice in case 4 has contracted a local network services management company to provide the necessary security policies, practices, mechanisms, and documentation for the practice to be in compliance. The approach to securing the information systems in all four cases is focused on HIPAA compliance and the state of security of the practices' information systems is the direct result of HIPAA compliance standards and requirements. The result of compliance driving system security was indicated by the Kwon and Johnson study involving hospitals. (Kwon & Johnson, 2013) See table for responses.

Table 17. Central Question Responses

Central Question	How compliant to the Security Rule of HIPAA and secure are information systems in the small medical and dental practices?
Case 1	Joined an integrated healthcare organization that provides the security policies, practices, mechanisms, and documentation for the practice to be in compliance
Case 2	Utilized an EHR cloud based solution where none of the patient's health records are resident at the practice and the solution provider is handling the compliance mandates to be in compliance.
Case 3	Engaged in every aspect of compliance by consistently following a guidance framework toolkit provided by the American Dental Association to be in compliance.
Case 4	Contracted a local network services management company to provide the necessary security policies, practices, mechanisms, and documentation for the practice to be in compliance.
Researcher	The approach to securing the information systems in all four cases is focused on HIPAA compliance and the state of security of the practices' information systems is the direct result of HIPAA compliance standards and requirements.

Commonalities:

There were a few commonalities discovered in the study. All four of the physicians and dentists expressed that they had to change the way they did business because of the compliance requirements to the HIPAA Security Rule and that is was an added expense to the practice. Also three of the four healthcare providers expressed feeling not fearful or as fearful on the non-compliance question but this situation could be the result of their solution decisions.

Differences:

There were a few differences among the four cases. One major difference was that each practice chose a different solution for HIPAA Security Rule compliance. Another difference is the choice for having the EHR physically reside at the practice's location. One of the physicians

and one of the dentists chose to keep their patients' records at the office. Also, the physicians' responses to the mandated compliance of the HIPAA Security Rule placed them either in the middle of the continuum or as an opportunity for the practice. While the dentists viewed the mandated compliance of the HIPAA Security Rule as a threat. Additionally, the physicians felt in control to the HIPAA compliance mandate while the dentists felt that they had no control.

Trends:

A number of trends have been identified by the case study. A new type of organization has emerged - the integrated healthcare organization. The integrated healthcare organization combines a number of healthcare providers such as hospitals, physicians groups, and other related healthcare providers into one multifaceted organization.

Another trend is the software as a service in the cloud for healthcare. This solution allows the healthcare provider to completely remove EHR from residing on the clinic's information system. This solution apparently alleviates the practice from most of the HIPAA Security Rule standards and requirements as long as the practice possess a business associates contract agreement stipulating that the solutions provider ensure that all HIPAA Security Rule standards and requirements are being met. Additionally, software application providers are offering industry and specialty specific solutions for a variety of healthcare organizations.

Also most of the professional organizations covering the various healthcare industries are providing their members with a selection of guidance framework toolkits having more focused instructional information and documentation for their particular industry or specialty within an industry or healthcare segment.

Additionally while only one of the four practices in the study allowed patients access to their personal health information on line, this service offering will continue to expand throughout the healthcare industry.

Potential Problems

A potential problem that should be addressed by the researcher is that the candidates that agreed to be participants in the study were eager to help in the research effort and were eager for the results of the study. While the study participants provided the information necessary for the study to be conducted, other potential participants may have provided different information. Also a very large number of physicians and dentists that were contacted were not interested in participating in the study. However, the participants in the study provided the information necessary for the researcher to gain an understanding and to enable the researcher to describe and discover the current state of information system security compliance of two medical and two dental practices based on the people, the procedures, and the technology involved in security compliance.

Suggestions for Future Research

The section from the study on management or the human perspective needs more focused and comprehensive research. The questions: How do the physicians'/dentists' primary and secondary appraisals to compelled compliance influence security compliance? and "How does the physicians' and dentists' fear of non-compliance influence security compliance?" should be explored and examined more thoroughly. Additionally, while Creswell suggested that 4 to 5 cases were a limit in case study research, there seems to be a rather wide range of possible

solutions to the medical and dental industries in helping them solve the problems related to HIPAA compliance.

Summary

The purpose of the case study research was to understand, describe, and discover the current state of information system security compliance of two medical and two dental practices based on the people, the procedures, and the technology involved in security compliance. The reasoning for selecting two different types of healthcare segments was to compare and to identify commonalities and differences, and to discover possible trends. It was a conjecture that since the medical offices and area hospitals share patient information, the medical offices were not only better informed than dental offices as to the importance of compliance and information system security practices but also more fearful of the repercussions for non-compliance. The research study accomplished gaining an understanding of the practices, has provided a description for each practice based on a number of issues, and has discovered the current state of information system security compliance based on the people involved, and the procedures, and the technology selected by the practices for HIPAA Security Rule compliance. It was discovered that there were a few commonalities among the practices and there were also a few differences. However, one of the major discoveries was that each practice chose a unique method for handling the HIPAA Security Rule compliance requirements. One chose to join a large integrated healthcare organization. Another chose to utilize a third party cloud application provider. The remaining two chose to purchase different EHR/practice management software solutions, but one chose to contract with a local network services management company to

provide their information system requirements and the other decided to handle their the information system requirements in house.

The study's original conjecture, that since the medical offices and area hospitals share patient information, the medical offices were not only better informed than dental offices as to the importance of compliance and information system security practices but also more fearful of the repercussions for non-compliance, did not pan out. All of the practices were equally informed as to the importance of HIPAA Security Rule compliance. Additionally based on the confidence in their chosen solutions, only one was fearful of non-compliance, but all felt confident in receiving positive results from an audit by the governmental agency.

The study discovered a number of trends including a new organizational structure, new types of application software and services, and the plethora of guidance information and documentation products offered by the various healthcare professional membership organizations to give small healthcare providers a wide range of compliance solutions from which to select the one that best suits their practice.

REFERENCES

American Recovery and Reinvestment Act (ARRA) of 2009, February 17, 2009, Pub. L. No. 111-5.

Beach, D. P., & Alvager, T. K. (1992). Handbook for scientific and technical research (1st ed.). Upper Saddle River, NJ: Prentice Hall.

Beaudry, A., & Pinsonneault, A. (2005, September). Understanding user responses to information technology: a coping model of user adaptation. *MIS Quarterly*, 29(3), 493-524.

Beaudry, A., & Pinsonneault, A. (2010, December). The other side of acceptance: studying the direct and indirect effects of emotions on information technology use. *MIS Quarterly*, 34(4), 689-710.

Clifford, M. (2004). Identifying and exploring security essentials. (1st ed.). Upper Saddle River, New Jersey 07458: Pearson Prentice Hall.

Conn, J. (2013, December 23). Gains, challenges abound for healthcare info tech. *Modern Healthcare*, 43(51), S36.

Creswell, J. W. (2013). Qualitative inquiry and research design: choosing among five approaches (3rd ed.). Thousand Oaks, CA: Sage Publishing.

Creswell, J. W. (2009). Research design qualitative, quantitative, and mixed methods approaches (3rd ed.). Thousand Oaks, CA: Sage Publishing.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2012, September). Future directions for behavioral information security research. *Computers & Security*, 32, 90-101.

DeGaspari, J. (2012, December 14). Healthcare providers face uphill battle in stemming data breaches. *Healthcare Informatics*, 30(1), 52.

Department of Health and Human Services, Centers for Medicare & Medicaid Services. (June, 2005: rev. March, 2007). HIPAA Basics of Risk Analysis and Risk Management. Retrieved January, 2011. Retrieved from https://www.cms.hhs.gov/EducationMaterials/.

Department of Health and Human Services, Centers for Medicare & Medicaid Services. (November, 2004: rev. March, 2007). HIPAA Security 101 for Covered Entities. Retrieved January, 2011. Retrieved from https:// www.cms.hhs.gov/EducationMaterials/.

Department of Health and Human Services, Centers for Medicare & Medicaid Services. (May, 2005: rev. March, 2007). HIPAA Security Standards Administrative Safeguards. Retrieved January, 2011. Retrieved from https:// www.cms.hhs.gov/EducationMaterials/.

Department of Health and Human Services, Centers for Medicare & Medicaid Services. (February, 2005: rev. March, 2007). HIPAA Security Standards Physical Safeguards. Retrieved January, 2011. Retrieved from https:// www.cms.hhs.gov/EducationMaterials/.

Department of Health and Human Services, Centers for Medicare & Medicaid Services. (May, 2005: rev. March, 2007). HIPAA Security Standards Technical Safeguards. Retrieved January, 2011. Retrieved from https:// www.cms.hhs.gov/EducationMaterials/.

Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of the American Recovery and Reinvestment Act of 2009. §13410(d).

Health Insurance Portability and Accounting Act (HIPAA) of 1996, August 21, 1996, Pub. L. No. 104-191.

Health Insurance Reform: Security Standards; Final Rule ("The HIPAA Security Rule"), 68 FR 8334, February 20, 2003. §164.308(a)(4).

HIPAA Security Rule Toolkit. (2011, November). Retrieve/download from http://www.scap.nist.gov/hipaa/.

Flick, U. (2009). An introduction to qualitative research (4th ed.). Thousand Oaks, CA: Sage Publishing.

Johnston, A. C., & Warkentin, M. (2010, September). Fear appeals and information security behaviors: an empirical study. *MIS Quarterly*, 34(3), 549-566.

Kaplan, B., & Maxwell, J. A. (1994, December). Qualitative research methods for evaluating computer information systems. *Management Information Systems Quarterly*, 12(4): 571-586.

Kumar, R. (2005). Research Methodology A Step-By-Step Guide for Beginners (2nd ed.) Thousand Oaks, CA: Sage Publications, Inc.

Kwon, J., & Johnson, M. E. (2013, Fall). Health care security strategies for data protection and regulatory compliance. *Journal of Management Information Systems*, 30(2), 41-65.

Marshall, C., & Rossman, G. B. (2011). Designing qualitative research (5th ed.). Thousand Oaks, CA: Sage Publications, Inc. Publishing.

Miles, M. B., Huberman, A. M., & Saldana, J. (2014). Qualitative data analysis: a methods sourcebook (3rd ed.). Thousand Oaks, CA: Sage Publishing.

Myers, M. D. (2013 updated 1997, September 3). Qualitative research in information systems. *MIS Quarterly*, 21(2), 241-242.

Pettigrew III, J. A., & Ryan, J. J. (2012, January/February). Making successful security decisions a qualitative evaluation. *Information Security Management* and co-published by the IEEE Computer and Reliability Societies, 60-68.

Rindfleisch, T. C. (1997, August). Privacy, information technology, and health care. *Communications of the ACM*, 40(8).

Rodriguez, L., (2013, September) Memorandum as Appendix B in Salmon, T.M. (2013, November) Department of Health and Human Services Office of Inspector General Report #A-04-11-05025. Retrieved from http://www.oit.hhs.gov/.

Rubin, H. J., & Rubin, I. S. (2012). Qualitative interviewing: the art of hearing data (3rd ed.). Thousand Oaks, CA: Sage Publishing.

Salmon, T.M. (2013, November) Department of Health and Human Services Office of Inspector General Report #A-04-11-05025. Retrieved from http://www.oit.hhs.gov/.

Sewart, J. M., Tittel, E., & Chapple, M. (2011). Certified information systems security professional study guide (5th ed.). Indianapolis, IN: Wiley Publishing, Inc.

Scholl, M., Stine, K., Hash, J., Bowen, P., Johnson, A., Smith, C.D. et al., (2008, October). An introductory resource guide for implementing HIPAA security rule. (NIST Special Publication 800-66) Retrieved February, 2011. Retrieved from http://csrc.nist.gov/publications.

Stevenson, G.W.P., & Valenta, A.L. (Fall, 2009) Securing ePHI an clinicians and IT ever agree? *Journal of Health Information Management* 23(4).

Stoneburner, G., Goguen, A., & Feringa, A., (2002, July). Risk management guide for information technology systems. (NIST Special Publication 800-30) Retrieved February, 2011. Retrieved from http://csrc.nist.gov/publications.

Verendel, V. (2009, September). Quantified security is a weak hypothesis: a critical survey of results and assumptions. Paper presented at NSPW'09: Proceedings of the 2009 Workshop on New Security Paradigms Workshop, Oxford, UK, 8-11 September (pp. 37 – 49). New York: ACM.

Volonino, L., & Robinson, S. R. (2004). Principles and practice of information security protecting computers from hackers and lawyers (1st ed.). Upper Saddle River, New Jersey 07458: Pearson Prentice Hall.

Yin, R. K. (2014). Case study research: design and methods (5th ed.). Thousand Oaks, CA: Sage Publishing.

APPENDIX A

MANAGEMENT QUESTIONS

Do you view the mandated compliance to the HIPAA Security Rule as an opportunity (or positive) to your practice or as a threat (or negative) to your practice? And Why?

Regarding the mandated compliance to the HIPAA Security Rule, do you feel that you have control in this situation or that you have no control in this situation? And Why?

On a scale of 1 to 5 with 1 feeling very high and 5 feeling very low, how would you rate your confidence in your current compliance situation if HHS showed up to perform an audit of your practice today? Why do you feel as you do regarding your confidence level?

On a scale of 1 to 5 with 1 feeling very fearful and 5 feeling very unafraid, how would you rate your concern over an HHS audit of your practice resulting in non-compliance?

Why?

In general, how does/has HIPAA compliance (Security Rule) impacted you and your practice?

How do your feel about it?

APPENDIX B

GENERAL COMPLIANCE QUESTIONS

Does your practice have policies and procedures in place for physical security and information system security?

Has your practice identified possible vulnerabilities and threats, and the resulting impact or risk to your practice?

Has your organization protected against all reasonably anticipated threats or hazards to the security and integrity of ePHI?

Has your organization analyzed these problems and created a mitigation plan that it is working to decrease risks and vulnerabilities?

Does your staff know how to handle physical security and information security issues with a lap top, PDA, tablet, smart phone, and/or other similar tools?

Does your staff know the importance of timely application of antivirus software and system patches to protect against malicious software and exploitation of vulnerabilities?

Does your practice monitor log-in attempts?

Does your practice have a procedure for reporting and handling security incidents?

Has your practice established a contingency plan that covers disaster recovery and back up?

Does any of your staff have the technical experience to evaluate your systems?

> If not -- Has your organization outlined the necessary factors to be considered in selecting an outside vendor, including credentials and experience?

Does your organization use a strategy and tool that considers all the elements of the HIPAA Security Rule, including all standards and implementation specifications?

Does your organization have business associate contracts and do your organization's agreements and other arrangements include security requirements meet all the HIPAA Security Rule requirements per the HITECH Act? Does your organization monitor physical access to the information system to detect and respond to physical security incidents?

Has your organization developed and implemented policies and procedures that address data back-up, data storage, and disposal of ePHI and / or the hardware and electronic media on which it is stored, including the appropriate methods to dispose of hardware, software and the data itself?

APPENDIX C

SPECIFIC TECHNICAL QUESTIONS

Access controls:

Do you or does your practice have access to technical policies and procedures?

Has your practice identified all applications, systems, servers and other electronic tools that hold and use ePHI?

Does your practice have an access control procedures policy that includes rules of user behavior and consequences for failure to comply and has this policy been communicated to your system users?

Does your practice have an electronic procedure that automatically terminates electronic session after a predetermined time of activity?

Does your practice have a process or mechanism to encrypt and decrypt ePHI?

Audit Controls:

Has your practice determined the appropriate scope of audit controls that are be necessary to protect your information systems and tools that contain ePHI based on your risk assessment?

Does your practice have an inventory of what systems, applications, processes, servers, laptops, PDAs, tablets (iPads) and other electronic tools make data vulnerable to unauthorized or inappropriate tampering, uses or disclosures of ePHI?

Does your practice have tools in place for auditing data review, creating, deleting and updating, plus for firewall system activity and other similar activities? For example: Can your organization trace all system activity, viewing, modifying, deleting and creating of ePHI, to a

specific user? Does your organization record each time ePHI is viewed, modified, deleted or created in an audit tool to support audit and other business functions?

Has your practice determined what are the most appropriate monitoring tools for your organization, such as third party tools, freeware, operating-system provided, or home grown?

Has your practice determined the type of audit trail data it will need, and the monitoring procedures to derive exception reports, other reports?

Integrity:

Does your practice have integrity policies and procedures?

Does your practice have a formally documented set of integrity requirements that is based on your analysis of use, users and misuses of ePHI and your risk analysis?

Does your practice have in place electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner?

Does your practice use authentication mechanisms, such as error-correcting memory, magnetic disc storage, digital signatures, check sum technology?

Does your practice's information integrity process provide a high level of assurance that information integrity is being maintained?

Person and Entity Authentication:

Does your practice have person and entity authentication policies and procedures?

Do your practice's identity methods corroborate that the person is the one claimed? What authentication methods does your organization use? For example: passwords, tokens, biometrics?

If your practice uses passwords for individual access to ePHI are they unique by individual?

Has your practice implemented the selected authentication methods into your organization's systems, networks, applications, and tools? (beyond initial user login?)

Does your practice use outside third party vendor support to implement your organization's authentication methods?

Transmission Security:

Does your practice have transportation policies and procedures that identify methods of transmission that will be used to safeguard ePHI and that identify tools and techniques that will be used to support the transmission security policy?

Does your practice have in place an auditing process during transmission that verifies that the ePHI has been protected against unauthorized access?

Has your practice implemented encryption for ePHI transmission?

APPENDIX D

NURSING/HYGIENSTS/OFFICE STAFF QUESTIONS

Does your organization use passwords?

Are these passwords unique by individual?

Are they kept in secret?

Does your organization have an electronic procedure that automatically terminates electronic session after a predetermined time of activity?

Have you been advised or trained on the clinic’s security policies and procedures covering electronic patient records?

Does your office use components such as a lap top, PDA, tablet, smart phone, and/or other similar tools?

If so, have you been advised or trained on how to handle physical security and information security issues with components?

Have you been advised or trained on the importance of timely application of antivirus software and system patches to protect against malicious software and exploitation of vulnerabilities?

Does your organization have business associate contracts and do your organization's agreements and other arrangements include security requirements?

How does/has the compliance mandate to HIPAA especially the Security Rule impact/ed you?

How do your feel about it?