2020

An Investigation of the Factors that Contribute to the Perceived Likelihood of Compliance with the HIPAA Security Rule among Healthcare Covered Entities and Business Associates

James Furstenberg

An Investigation of the Factors that Contribute to the Perceived Likelihood of Compliance with the HIPAA Security Rule among Healthcare Covered Entities and Business Associates

by
James J. Furstenberg

A dissertation submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
in
Information Assurance

College of Computing and Engineering
Nova Southeastern University

2020

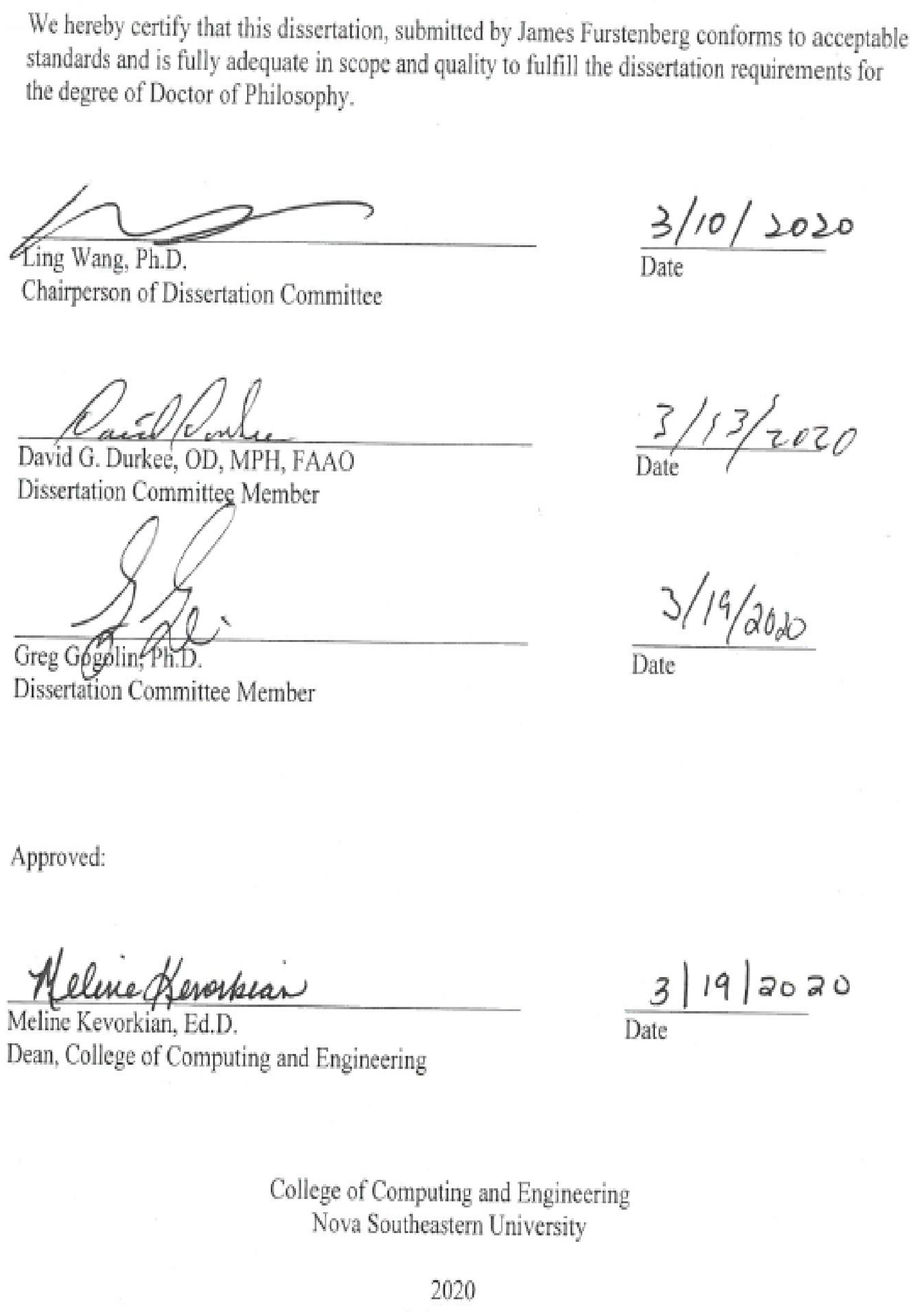
An Abstract of a Dissertation Submitted to Nova Southeastern University in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

An Investigation of the Factors that Contribute to the Perceived Likelihood of Compliance with the HIPAA Security Rule among Healthcare Covered Entities and Business Associates

by
James J. Furstenberg
February 2020

The Health Insurance Portability and Accountability Act (HIPAA) Security Rule (SR) mandate provides a national standard for the safeguard of electronically protected health information (ePHI). SR compliance enforcement efforts started in 2005; however, U.S.-based covered entities and business associates (CEs & BAs) remain challenged to comply with the HIPAA SR regulatory strategy. Although there is a significant volume of academic research on HIPAA compliance, research specific to the SR is sparse.
This study addressed the research gap by designing a unique conceptual model that assessed factors affecting CEs & BAs compliance (or non-compliance) with the SR regulatory strategy. The primary goal of this research study was to develop and empirically measure how motive, characteristics and capacity, regulator respect, and deterrence factors impacted the perceived likelihood of compliance with HIPAA SR in healthcare CEs & BAs operating in the United States. Multiple linear regression determined whether motive, characteristics and capacity, regulator respect, or deterrence factors better predicted the perceived likelihood of compliance with HIPAA SR, rather than any single factor alone. Only characteristics and capacity were a statistically significant predictor of the perceived likelihood of compliance. Motive and characteristics and capacity were significantly and positively correlated with the perceived likelihood of compliance with HIPAA SR. A negative correlation existed between the perceived likelihood of compliance with HIPAA SR and deterrence factors. There was no correlation between a perceived likelihood of compliance with HIPAA SR regulator respect. This research contributes toward filling the previous knowledge gap and providing insight into the factors and challenges CEs & BAs face in meeting compliance mandates.

Approval and Signature



We hereby certify that this dissertation, submitted by James Furstenberg conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.

3/10/2020

Ling Wang, Ph.D. — Date
Chairperson of Dissertation Committee

David Durkee — 3/13/2020

David G. Durkee, OD, MPH, FAAO — Date
Dissertation Committee Member

3/19/2020

Greg Gogolin, Ph.D. — Date
Dissertation Committee Member

Approved:

Meline Kevorkian — 3|19|2020

Meline Kevorkian, Ed.D. — Date
Dean, College of Computing and Engineering

College of Computing and Engineering
Nova Southeastern University

2020

Acknowledgments

"*All knowledge without Christ was vain*" Founders of Harvard College.

This dissertation has been a walk of faith. To my LORD and Savior, Jesus Christ, you gave me strength when I was weak, you gave me courage when I was afraid, and you gave me rest when I was exhausted. All praise, honor, and glory for this work are reserved solely for you.

I want to thank my family. Mandi, my wife, for your selflessness, continual sacrifices, and love; without it, I would have never survived. Jamie, my daughter, for your clinical research expertise, and mastery of the English language, I am forever grateful. To Jesse, my son, your mathematical prowess, has bailed me out many times over my educational journey. To my mom and dad, you are always a constant inspiration for me.

Throughout this experience, I have been continuously humbled by the support of friends and the kindness of strangers. To Dr. James Brady, Dr. Christine Nielson, and Dr. Nancy Martin, your kindness, permission, and pioneering research in compliance energized this research. To Dr. David Durkee, thank you for your support, advice, and kindness.

To Bob and Mary Chaput, whom I am honored to call my friends. Your kindness and support of my research were critical in reaching my Ph.D. dream; your kind-heartedness will never be forgotten. To the company you founded, Clearwater Compliance and all its employees who have made it the epitome of a first-class compliance and cybersecurity operation, thank you for your help and support over the years.

I want to thank Dr. Greg Gogolin, my mentor, friend, and fellow educator. Since our first meeting in 2005, you have been instrumental and an inspiration in my professional and personal growth. I have immense respect and gratitude for the life-changing journey you have provided, and for all the advice. You have had my back every step of the way. I strive to model the positive impact you have had on me to my students.

Finally, to Dr. Ling Wang, one could not find a better chair. Thank you for your guidance and, more importantly, for caring about students. Without you, this would not have been possible. Your kindness and student-centered focus are a model that I seek to have with my students. Words will never express what your caring has meant to my wife, and me. Thank you for everything. You are a first-class educator, whom I have the pleasure of calling my friend.

"I will ever walk humbly before my GOD, and meekly, mildly, and gently towards all men...to give myself- my life, my wits, my health, my wealth - to the service of my GOD and Savior"   John Winthrop

Table of Contents

Chapters

List of Tables

Tables

List of Figures

Figures

Chapter 1

Introduction

Background

The Health Insurance Portability and Accountability Act (HIPAA) Security Rule (SR) regulatory strategy and mandate provide healthcare covered entities and business associates (CEs & BAs) national standards for the protection of highly sensitive electronic protected health information (ePHI) (Bilimoria, 2009). The enactment of the 1996 HIPAA statute §160.103 defined a *healthcare covered entity* as "(1) A health plan; (2) a healthcare clearinghouse; (3) a healthcare provider who transmits any health information in electronic form" (U.S. Department of Health and Human Services (HHS), 2003, p. 8337). Additionally, statute §160.103 defined a *business associate* as "any person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of or provides services to, a covered entity" (HHS, 2013, p. 1). CEs & BAs are federally mandated to comply with the SR standards (HIPAA, 2011).

The SR standards were designed to protect the confidentiality, integrity, and availability of ePHI that is accessed, stored, transmitted, and received (HHS, 2013). The SR regulatory strategy attempts to institute a set of technical and non-technical security controls, and implementation specifications collectively called safeguards that CEs &

BAs are required to apply and address (HHS, 2013). However, despite HIPAA law being enacted in 1996, there appears to be little improvement in SR compliance among CEs & BAs (G. Cohen & Mello, 2018; L. T. Cohen, 2016; Sanches, 2017; U.S. Department of Health and Human Services Office for Civil Rights (OCR), 2018c).

To date, compliance with the SR standards and the operationalization of the SR regulation strategy remains a challenge for CEs & BAs (Donavan, 2018; Healthcare Information and Management Systems Society (HIMSS), 2018; (OCR, 2018a). Subsequently, most CEs & BAs are only moderately confident that their organization would be prepared for a HIPAA compliance audit (SAI Global, 2017). Moreover, the Office for Civil Rights (OCR), the U.S. government agency charged with HIPAA compliance oversight, compliance audits, and breach investigations consistently reveal that CEs & BAs remain slow to adopt the SR regulatory strategy and fulfill SR compliance mandates (Donavan, 2018; Gallagher, 2016; Sanches, 2017).

Failure to comply with the SR regulatory mandates leaves the healthcare industry highly vulnerable to OCR compliance audits and investigations. These noncompliance acts can result in substantial civil monetary penalties, sanctions, and, ultimately, the loss of licensure (Alder, 2017; U.S. Department of Health & Human Services, 2015)(OCR, 2018b). Additionally, CEs & BAs may be subject to criminal prosecution if they fail to properly secure ePHI (Alder, 2017; Stevens, 2009). HIPAA non-compliance fines are on the rise, with the HIPAA Journal (2017) reporting 2017 as another record-breaking year for HIPAA non-compliance fines. These ongoing issues serve to show that the healthcare industry remains challenged to adopt and comply with the SR regulatory strategy and compliance mandates.

The SR has been in force since 2005, and yet CEs & BAs continue to struggle with compliance activities and to adopt the current SR regulatory strategy (Sanches, 2017). McLeod and Dolezel (2018) recognized that no standard exists for CEs & BAs to measure up to, or to ensure compliance with the SR. It is, therefore, critical to investigate the SR compliance of CEs & BAs to ascertain factors impacting compliance with the SR regulatory strategy. While CEs & BAs struggle to comply with regulations that were designed to safeguard and protect highly sensitive and private ePHI, cybercriminals have realized just how vulnerable and profitable the healthcare industry can be (Fortinet, 2018).

Security vendor Fortinet's (2018) fourth-quarter report stated healthcare is experiencing twice the number of cyber-attacks (32,000 intrusion attacks per day) as compared to other industries (14,300 intrusion attacks per day) in the same vertical market sector. These attacks are troubling because healthcare data breaches are consistently high in terms of volume, frequency, impact, and cost in comparison to other industries (Ponemon Institute, 2016). Furthermore, in the past two years, nearly 90 percent of all healthcare entities have suffered a data breach in some form (Blackbook Market Research LLC., 2018). While cyber breaches can occur for many reasons, there is overwhelming evidence that internal process breakdowns, perceived compliance, lack of security controls, and other non-nefarious actions are the largest contributors to healthcare data breaches (HIMSS, 2018).

Ponemon Institute's (2016) healthcare breach report stated that the average cost of a healthcare data breach is more than $2.2 million. Moreover, in just three short years, Ponemon Institute's (2019) breach cost report stated that healthcare breach costs had risen substantially. Ponemon Institute's (2016) report indicated that healthcare is spending more than all other sectors (60%), and for the ninth consecutive year, breach cost has risen to $ 6.5 million on average. Understandably CEs & BAs are under constant pressure to defend against cyber breaches, and yet the healthcare industry is replete with a long history of SR noncompliance (Alder, 2017). With all these factors threatening CEs & BAs, there is an urgent need for practical and empirically based SR compliance research.

An overview of the previous literature reveals limited research devoted to the SR (Angst, Block, D ’Arcy, & Kelley, 2017; Martin, Imboden, & Green, 2015). Past research studies have purported various theoretical frameworks and conceptual models to help understand overall HIPAA compliance, or the lack thereof, in CEs & BAs. However, it appears that research specific to the SR is sparse (Duncan & Whittington, 2014; Martin et al., 2015). Existing research is limited to non-operationalized theoretical models; i.e., Martin et al. (2015) (Appendix A, Figure A1), or single theoretical approaches toward explaining compliance behaviors, intentions, and perceptions (Gaia, Wang, Basile, Sanders, & Murray, 2018; Kuo, Chen, Talley, & Huang, 2018; Zhang & Zhang, 2018). Disagreement exists within the research community as to the efficacy of research that uses a single one theoretical approach to investigate highly complex topics, like regulatory compliance (Losoncz, 2017).

Previous research purported that factors, such as employee motive, are foundational to understanding an organization’s compliance (Nielsen & Parker, 2012; Vance, Siponen, & Pahnila, 2012). However, others researchers have stated that an organization needs the characteristics and capacities (business model, knowledge of SR rules, the capacity to comply, budget, expertise, and management support) to be able to comply (Anthony, Appari, & Johnson, 2014; Appari, Anthony, & Johnson, 2006; Nielsen & Parker, 2012; Vance et al., 2012). An organization’s employees may be motivated to comply, but without the characteristics and capacities, compliance toward a regulatory strategy will still be an issue (Brady, 2010; J. Chen & Benusa, 2017).

Deterrence and deterrence theory has been previously used to explain the effects of sanctions, and sanction severity, on regulatory compliance behaviors, intentions, and perceptions of compliance (X. Chen, Wu, Chen, & Teng, 2018; Gaia et al., 2018). However, there appears to be disagreement as to whether or not deterrence factors ultimately motivate regulatory compliance in an organization. Some have proposed regulatory relationships, and regulator respect affects an organization’s willingness to comply (Alzahrani, Johnson, & Altamimi, 2018; Parker & Nielsen, 2011). Furthermore, non-compliance sanctions and sanction severity may be subjective, based on the regulator’s relationship with an organization (Alzahrani et al., 2018). This research study investigated the factors of motive, characteristics and capacity, regulator respect and deterrence factors of U.S. based healthcare CEs & BAs and the perceived likelihood of complying with the HIPAA SR regulatory strategy.

Problem Statement

This research study investigated compliance perceptions in CEs & BAs operating in the U.S., to explore why they remain challenged to comply with the HIPAA SR regulatory strategy (Holtzman, 2017; Litten, 2017; Mohammed, Mariani, & Mohammed, 2015; Rodriguez, 2013; Sanches, 2017; U.S. Department of Health and Human Services Office for Civil Rights (OCR)., 2018d). Academic research has provided insight into complex issues, such as behavioral and attitudinal responses toward SR compliance regulatory strategy (Drahos, 2017c). However, comprehensive academic research, investigating SR regulatory compliance perceptions and attitudinal responses, is sparse (Angst et al., 2017; M. Gold & McLaughlin, 2016; Hawthorne & Richards, 2017; Hoffman & Podgurski, 2006; Martin et al., 2015). Most of the existing literature focuses on the HIPAA privacy rule (Brinkman, 2019), overall HIPAA compliance (Benitez & Malin, 2010; Shindell, 2016), larger medical centers (J. Chen & Benusa, 2017), or smaller and specific types of medical centers, i.e., academic medical centers (Brady, 2010; Primeau & Debra, 2017). Martin et al., (2015) recognized that research regarding the SR is insufficient, with little explanation as to why HIPAA SR compliance or non-compliance challenges, in CEs & BAs, still exist.

Empirically based SR research that identifies and assesses factors relating to compliance with the current SR regulatory strategy is critical. Compliance of CEs & BAs, and their perceptions of compliance are also important (G. Cohen & Mello, 2018; L. T. Cohen, 2016; Donavan, 2018; Healthcare Information and Management Systems Society (HIMSS)., 2018). Research specific to SR compliance would provide essential data in an area of scant SR research (Martin & Imboden, 2014; Sanches, 2017). This research study examined how the SR regulatory strategy impacts CEs & BAs and generated data to increase a currently limited body of SR regulatory compliance knowledge (Cannoy & Salam, 2010).

Parker and Nielsen (2011) identified that previous regulatory compliance research had taken an objectivist or an interpretivist theoretical approach. Theories formulated with either of these paradigms provided a lens in which to view, explain, and predict compliance phenomena (Johnson, Onwuegbuzie, & Turner, 2007). Objectivistic theoretical approaches focus on building models and seek to identify the external and internal factors associated with non-compliance or compliance (Charmaz, 2000; Parker & Nielsen, 2011). Whereas, an interpretivist approach, is more concerned with the regulatees thoughts, perceptions, and accepted reality, as well as their experience structure (Kingsbury, 1997). Although single theoretical approaches have their advantages, they also confuse and often present conflicting results in regulatory and compliance research (Losoncz, 2017). Therefore, a single approach may not be enough for deeply complex challenges like that of regulatory and compliance research (Losoncz, 2017).

Compliance research is complicated, challenging to perform, and problematic to design (Drahos, 2017a; Parker & Nielsen, 2011). Currently, investigating organizational responses to regulatory strategy is an active area for theoretical development (Parker & Nielsen, 2011). Building robust theories and hypotheses is foundational to understanding compliance and regulatory strategy that seek to explain factors affecting compliance or non-compliance (Parker & Nielsen, 2011). Bagozzi (2011) stated that the formulation of theories and hypotheses, as well as testing them, is the central goal in organizational and information systems (IS) research. However, Losoncz (2017) stated that there are few published studies regarding integrative research paradigms (objectivist and interpretivist) in regulatory compliance research. Because integrative regulatory research paradigms are sparse, numerous theoretical perspectives have been proposed, creating discrepancies between disciplines and methodological approaches toward understanding regulatory compliance (Drahos, 2017c).

A compliance research approach that purposely seeks to integrate both (objectivistic and interpretivist) paradigms is considered to be more inclusive and holistic (Danermark, Ekstrom, & Jakobsen, 2005; Parker & Nielsen, 2011, 2017). Integrating both theoretical frameworks and designing a holistic conceptual model is necessary in order to study complex, challenging, and vital issues, such as regulatory compliance (Losoncz, 2017). Integrating varied paradigms into a single research study has been purported to be the best way to understand the complexities and factors that affect compliance with the regulatory strategy (Drahos, 2017c).

A holistic conceptual model's research design may assist in understanding the factors affecting CEs & BAs compliance, or non-compliance, with the SR regulatory strategy (Drahos, 2017b; Parker & Nielsen, 2010). Moreover, a holistic model may provide the framework to gather the necessary information about possible reasons why CEs & BAs have trouble complying with the SR regulatory strategy (Parker & Nielsen, (2017). This research study developed a unique and holistic SR compliance conceptual model that investigated motive, characteristics, and capacity, regulator respect, as well as deterrence factors in U.S. based healthcare CEs & BAs and how they related to the perceived likelihood of complying with HIPAA SR.

Dissertation Goal

The goal of this research study was to develop and empirically assess a unique conceptual model toward predicting the effect of motive, characteristics and capacity, regulator respect, as well as deterrence factors toward U.S. based healthcare CEs & BAs perceived likelihood of complying with the HIPAA SR. To investigate this goal, a unique conceptual model was developed, using a holistic approach (Parker & Nielsen, 2011).

Parker and Nielsen (2011) purported that holistic theoretical model of business compliance (Appendix B, Figure B1), along with 14 dimensions of compliance, (Appendix C, Figure C1), provide an all-encompassing approach toward investigating compliance or non-compliance issues in regulatory research. Parker and Nielsen (2011) unique contributions and work in the regulatory and compliance fields are well known and well respected (Drahos & Krygier, 2017). The Parker and Nielsen (2011) theoretical model and it's 14 dimensions were derived from an extensive review and synthesis of regulatory, as well as compliance research from business, legal, and environmental domains (Parker & Nielsen, 2017).

Parker and Nielsen (2011, 2017) stated that the 14 dimensions could serve as a guide in developing survey questions and survey instruments for investigating compliance. Moreover, the 14 dimensions may help uncover information about a targeted group's acceptance, preceptions, and compliance posture with a regulatory strategy (Parker & Nielsen, 2017). Parker and Nielsen (2017) stated that the use of all 14 dimensions might help support the thoroughness of compliance research by serving as a checklist of crucial issues.

Appendix C, Figure C1 illustrates Parker and Nielsen (2017) 14 dimensions of compliance. This research study leveraged and modified the original 14 dimensions from Parker and Nielsen (2017), with permission, to develop and design a holistic conceptual model and survey instrument that assessed SR compliance perceptions in U.S. based healthcare CEs & BAs. Modification of the 14 dimensions for survey questions was necessary to provide measures for SR compliance, as these dimensions were developed from the business, legal, and environmental domains. This research study is the first to integrate the 14 dimensions into the healthcare domain. As mentioned, permission to adapt, extend and modify Parker and Nielsen (2017) 14 dimensions can be seen in Appendix D, Figure D1.

Furthermore, this research study extended and operationalized the HIPAA SR theoretical framework purported by Martin et al. (2015). Martin et al. (2015) theoretical frameworks' s model (Appendix A, Figure A1), purported that resource capacity, enforcement environment, and organizational factors, as well as social and normative pressures, may influence HIPAA SR noncompliance behaviors. Martin et al. (2015) theoretical framework identified similar factors to those used in this research. However, Martin et al. (2015) theoretical framework' s model only focused on smaller healthcare organizations and never actually conducted any empirical assessment or testing of the model.

Martin et al. (2015) granted permission for the extension and operationalization of their model. Furthermore, Martin et al. (2015) stated that it is not a complete framework, but one where future researchers can expand, adapt, and use to aid in the empirical testing of HIPAA SR compliance perceptions and behaviors. Permission to adapt, extend Martin et al. (2015) theoretical framework is in Appendix E, Figure E1.

Figure 1 illustrates the holistic conceptual model, along with the 14 dimensions utilized in the constructs developed for this research study. Figure 1's unique holistic conceptual framework served as a model for investigating motives, characteristics, and capacities, regulator respect and deterrence factors impact the perceived likelihood of complying with the HIPAA SR (Drahos, 2017b; Nielsen & Parker, 2012; Parker & Nielsen, 2011).

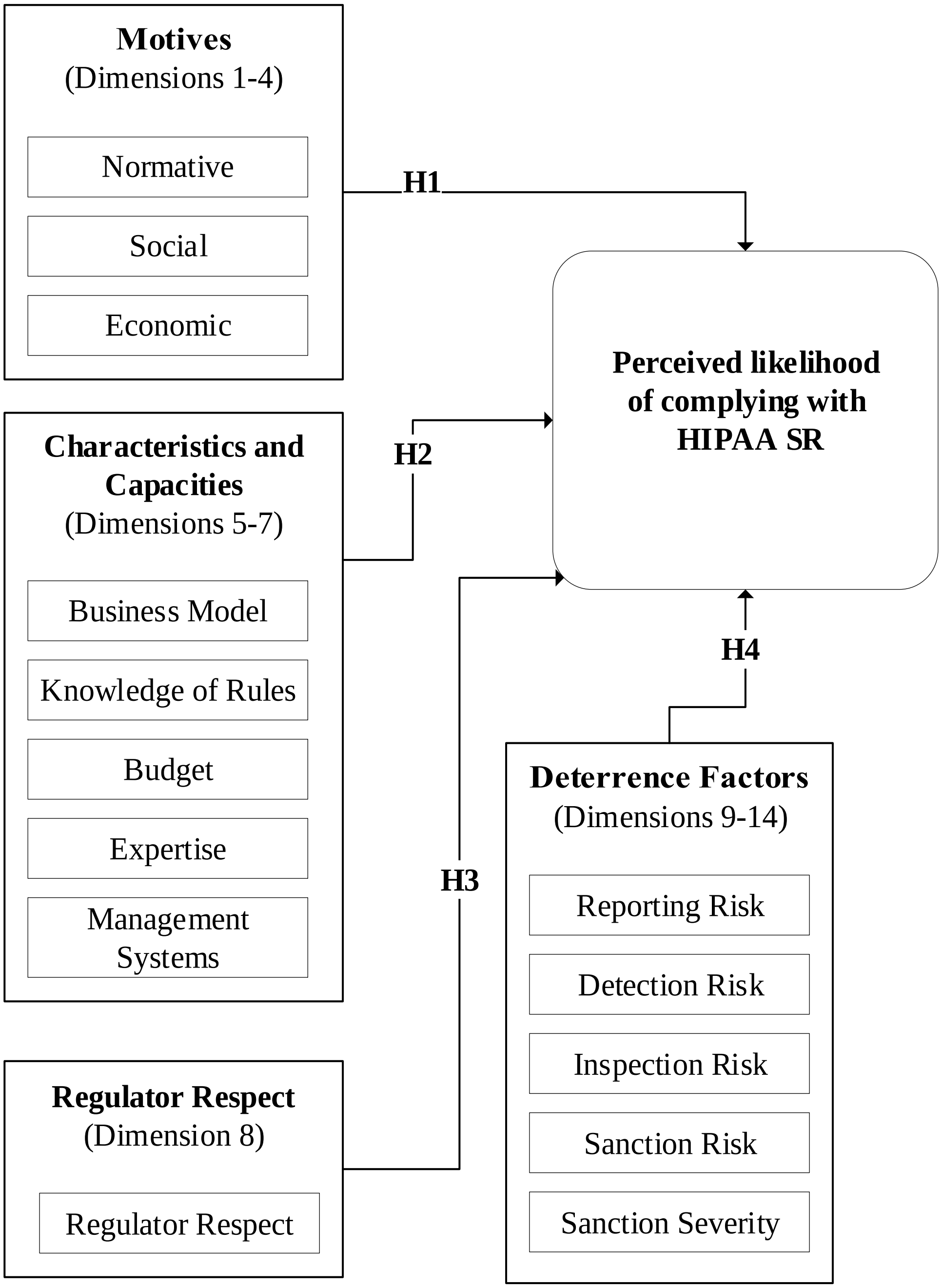


Figure 1. Holistic Conceptual Model with 14 Dimensions. Adapted with permission (Martin et al., 2015; Parker & Nielsen, 2011,2017) for use as the conceptual model of factors and their effect on the perceived likelihood of complying with HIPAA SR in healthcare CEs & BAs operating in the U.S.

Figure 1 includes the independent variables (IVs) and the dependent variable (DV) as well as their related dimensions of:

(a) Motive (MT) - (Alzahrani et al., 2018; Bulgurcu, Cavusoglu, & Benbasat, 2010; Kuo et al., 2018; Nielsen & Parker, 2012; Parker & Nielsen, 2017; Treekrutpant, 2017; Vance et al., 2012);

(b) Characteristics and Capacities (CC) - (Angst et al., 2017; Brady, 2010; J. Chen & Benusa, 2017; Nielsen & Parker, 2012; Parker & Nielsen, 2017);

(c) Regulator Respect (RR) - (Parker & Nielsen, 2010, 2011, 2017);

(d) Deterrence Factors (DT) - (X. Chen et al., 2018; Gaia et al., 2018; Gunningham, 2010; Parker & Nielsen, 2017; Weistroffer, 2016);

and the dependent variable (DV);

(e) Perceived likelihood of Compliance (PC1) with the HIPAA SR (Brady, 2010; Johnston & Warkentin, 2008; Martin et al., 2015; McLeod & Dolezel, 2018; Parker & Nielsen, 2010).

Appendix F, Tables F1-F5 illustrate a modified list of Parker and Nielsen (2017) 14 dimensions, which provided the foundation for the aforementioned conceptual model, including constructs that served in the development of survey instruments. Appendix F, Tables F1 - F5 are organized by the independent variables (IVs) (a) motive (MT) (Appendix F, Table F1), (b) characteristics and capacities (CC) (Appendix F, Table F2), (c) regulator respect (RR) (Appendix F, Table F3), and (d) deterrence factors (DT) (Appendix F, Table F4), along with the dependent variable (DV) perceived likelihood of compliance (PC1) (Appendix F, Table F5). Moreover, Appendix F provides the constructs, survey questions, and literary references used to support construct development. This research study's holistic approach and unique theoretical model have provided insight into factors, actors, and social interactions that exist in SR regulatory compliance research (Losoncz, 2017; Parker & Nielsen, 2011, 2017).

Research Question

The research question was:

RQ: Do the factors of (a) motives; (b) characteristics and capacities; (c); regulator respect and (d) deterrence predict the perceived likelihood of compliance with the HIPAA SR among healthcare CEs & BAs operating in the U.S?

Hypotheses

Any research goal regarding compliance and regulatory strategy requires the formulation of a good explanatory theory and generation of hypotheses (Bagozzi, 2011). Testing of a theory becomes the cornerstone in building a solid understanding of the factors that contribute toward or detract from compliance to a regulatory strategy (Parker & Nielsen, 2011). This research study was based on the development and empirical assessment of a unique and holistic conceptual model, and examined how (a) motives, (b) characteristics and capacities, (c) regulator respect and, (d) deterrence factors interact with the perceived likelihood of complying with the HIPAA SR. Subsequently, the hypotheses developed for this study were:

H1: Motive is a significant predictor toward the perceived likelihood of complying with HIPAA SR in CEs & BAs.

H2: Characteristics and capacities are a significant predictor toward the perceived likelihood of complying with HIPAA SR in CEs & BAs.

H3: Regulator respect is a significant predictor toward the perceived likelihood of complying with HIPAA SR in CEs & BAs.

H4: Deterrence is a significant predictor toward the perceived likelihood of complying with HIPAA SR in CEs & BAs.

This research study defined the four independent variables based on Parker and Nielsen (2017) 14 dimensions of compliance. Appendix F, Table F1, illustrates a pluralistic definition of motive (MT), that included economic, social, and normative phenomena (Parker & Nielsen, 2017). Economic motive was considered to be the cost, or benefit, as it related to CEs or BAs monetary utility (Nielsen & Parker, 2012). The normative motive provided an assessment of commitment to do the right thing and general belief in abiding by the law (Nielsen & Parker, 2012). Social motive assessed the influence that non-official parties have on CEs & BAs compliance activities (Nielsen & Parker, 2012). The mixed definition of motive offered the ability to assess whether compliance fits with business goals or detracts from them (Nielsen & Parker, 2012). Appendix F, Table F1, illustrates the motive survey question(s) MT1-MT3 that were included in the survey instrument.

Table F2, Appendix F illustrates a pluralistic definition of characteristics and capacities (CC), which includes (a) business model, (relevancy of compliance to business), (b) knowledge of SR rules, and (c) capacity to comply (budget, expertise, time and, management support) (Parker & Nielsen, 2017). An organization’s business model is vital to compliance (Drahos, 2017a). If regulatory obligations are perceived to be irrelevant to the business, then compliance is less likely (Parker & Nielsen, 2017). CEs & BAs need to be aware of SR mandates and have the capacity to understand them in order to comply fully (Tipton & Nozaki, 2011). The capacity to comply is based on budget, expertise, time, and management support (Angst et al., 2017). Parker and Nielsen (2009) purported that commitment of budget, expertise, time, and management support are essential factors for an organization's compliance practices. Table F2, Appendix F shows the characteristics and capacities constructs and survey question(s) CC1-CC8 used to assess the IV of CC empirically.

Table F3, Appendix F, shows the regulator respect (RR) construct. The RR dimension may influence the belief in the regularity fairness, legitimacy, and seriousness of audit and enforcement efforts (Parker & Nielsen, 2017). Also, respect for the regulator may influence the way CEs & BAs perceive all 14 dimensions (Parker & Nielsen, 2017). The RR survey question(s) RR1-RR3 can be seen in Table F3, Appendix F.

Table F4, Appendix F, shows deterrence factors (DF) constructs. CEs & BA's perception of regulatory enforcement, likelihood, and risk of inspection, detection as well as the severity of sanctions play a role in an organization's willingness to comply with regulatory strategy (X. Chen et al., 2018). Parker and Nielsen (2017) purported that perception of risk is stronger than the actual reality of deterrence factors in terms of its influence on regulatees. DT survey question(s) DT1-DT10, can be seen in Table F4, Appendix F.

Table F5, Appendix F, shows a new dimension, dimension 15. Dimension 15 was developed to measure the perceived likelihood of compliance (PC1) to the SR (X. Chen et al., 2018; Wall, Lowry, & Barlow, 2016). The PC1 survey dimension, and related measure, was used to understand better how CEs & BAs perceived the likelihood of SR compliance in their organization. What was the perceived level of assurance, among CEs & BAs, that they were fully compliant to the SR?

Relevance and Significance

Research exists to investigate and explore complex phenomena like that of regulatory compliance (Leedy & Ormrod, 2019). Research can help diagnose situations and create new ideas toward explaining a phenomenon (Zikmund, Babin, Carr, & Griffin, 2013). Researchers should not be deterred in attempting to quantify the unquantifiable; in this case, SR compliance in CEs & BAs, while full well acknowledging that it is a research path very few want to travel (Drahos, 2017; Parker & Nielsen, 2010, 2017).

Drahos (2017), Nielsen and Parker (2012), as well as Parker and Nielsen (2017), have called for future research to examine motives and other factors that influence compliance. This research study developed and tested a unique conceptual model to examine SR compliance. Parts of the theoretical framework, purported by Martin et al. (2015), was operationalized and extended (with permission of the author) for this research study (Appendix A, Figure A1).

Martin et al. (2015) theoretical framework model (Appendix A, Figure A1) reported that resource capacities, enforcement environment, organizational factors, and social and normative pressures, may influence HIPAA SR noncompliance behaviors. However, that theoretical frameworks' s model focused solely on smaller healthcare organizations and was never tested (Martin et al.,2015). Martin et al. (2015) granted permission for the extension and operationalization of their model (See Appendix E, Figure E1). Furthermore, Martin et al. (2015) stated that it is not a complete framework, but one that can be expanded upon, adapted, and used to test HIPAA SR compliance perceptions and behaviors empirically.

Barriers and Issues

There are several challenges with empirical research investigating regulatory compliance. In research of this nature, the researcher determines and predefines compliance as a fixed variable and then develops a strategy to measure it (Drahos, 2017a). Furthermore, the measurement, strategy, and definition must be defensible and realistic (Parker & Nielsen, 2011). This research study performed an extensive literature review and developed a measurable, reasonable, and defensible definition of the dependent variable (DV).

Compliance research can be challenging, as much of the data required is highly sensitive. Delving into an organization’s security, risk operations, and management may expose previously unknown problems (Parker & Nielsen, 2010). Sensitivity and pragmatism to this issue caused this research study to focus on the perceived likelihood of complying with the SR, not the direct observation of compliance, which created an environment more conducive for participation (Fowler, 2014).

Participant recruitment is always a challenge in compliance research, as the ability to access a target population is difficult. This study sought to include participants with authority to respond to compliance-related survey questions (Parker & Nielsen, 2010). The help of a project champion aided this research study. The project champion was instrumental in identifying participants and served as the primary distributor of the Security Rule Compliance (SRC) survey instrument.

Reaching an adequate population sample size was challenging due to the specificity and sensitivity of the research study’s topic and focus: SR compliance. An anonymous, web-based survey was used in order for the SRC survey instrument to be efficiently distributed. This survey format afforded the ability to reach more participants, and its anonymity was thought to help increase a participant's willingness to respond. As such, the calculated population sample size was reached (Nardi, 2018a).

Assumptions

This research study assumed that all participants answered honestly, and checks for SRC survey completeness were in place, such as requiring responses (Ellis & Levy, 2009). An adequate population sample size and the number of completed surveys were obtained within the designated time period.

Limitations

The generalizability of this research study is to be limited to SR compliance in CEs & BAs operating within the U.S. This research study used a web-based survey instrument, which may have include bias errors, such as sample frame and non-response bias (Fowler, 2014).

Delimitations

This research study was limited to the constructs of (a) motive (MT), (b) characteristics and capacities (CC), (c) regulator respect (RR), and (d) deterrence factors (DT), as they related to the perceived likelihood of complying with HIPAA SR (PC1). Furthermore, the topic and population scope of this research study were restrictive, only including perceptions of HIPAA SR compliance among CEs & BAs operating in the United States.

Definition of Terms

Business Associate – “ any person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity” (U.S. Department of Health & Human Services (HHS), 2013, p. 1).

Corrective Action Plans – “legally required compliance remediation actions, security control implementation(s) and other performance over time mitigation activities” [identified because of a breach investigation or OCR compliance audit] (OCR, 2018b, para 1).

Delphi Expert Technique – “involves the repeated individual questioning of the experts (by interview or questionnaire) and avoids confrontation of the experts with one another” (Dalkey & Helmer, 1963, p. 458).

Electronic Protected Health Information (ePHI) - “information that comes within paragraphs (1)(i) or (1)(ii) of the definition of protected health information as specified in this section”. The definitions are indicated within these paragraphs, it specifies information 1(i) “transmitted by electronic media” and 1(ii) “maintained in electronic media” (HIPAA, 1996, p. 8374).

Health Insurance Portability and Accountability Act of 1996 (HIPAA) – “directed Department of Health and Human Services [HHS] to adopt standards to facilitate the electronic exchange of health information for certain financial and administrative transactions. Health plans, healthcare clearinghouses, and healthcare providers are required to use standardized data elements and comply with national standards and regulations. Failure to do so may subject the covered entity to penalties” (Stevens, 2009, p. i).

Healthcare Covered Entity - any health plan, healthcare clearinghouse or healthcare provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter “ (HIPAA, 1996, p. 979).

Health and Human Services – “also known as the Health Department, is a cabinet-level department of the U.S. Federal Government with the goal of protecting the health of all Americans and providing essential human services” (HHS, n.d., para 1).

Implementation Specification - is an additional detailed instruction for implementing a particular [Security Rule] standard” (HHS, 2007, p. 5).

Office for Civil Rights – a department inside the U.S. Department of Health and Human Services (HHS) organization that “enforces federal civil rights laws, conscience, and religious freedom laws, the Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security, and Breach Notification Rules, and the Patient Safety Act and Rule, which together protect your fundamental rights of nondiscrimination, conscience, religious freedom, and health information privacy” (OCR, 2018a, p. para 1).

Protected Health Information - “Protected health information means individually identifiable health information: [Except as provided in paragraph (2)] that is:

(i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium. (2) Protected health information excludes individually identifiable health information: (i) In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; (ii) In records described at 20 U.S.C. 1232g(a)(4)(B)(iv); (iii) In employment records held by a covered entity in its role as employer; and, (iv) Regarding a person who has been deceased for more than 50 years"(HIPAA, 1996, pp. 983–984).

Required Implementation Specification – "the covered entity must implement policies and/or procedures that meet what the [Security Rule] implementation specification requires" (HHS, 2007, p. 5).

Risk Analysis – "Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the organization" (HHS, 2011, p. 734).

Safeguard Categories – "security [rule] standards are divided into the categories of administrative, physical, and technical safeguards" (HHS, 2007, p. 8).

Security Risk Assessment- "[i]mplement policies and procedures to prevent, detect, contain, and correct security violations"(CMMS., 2007, p. 2)

Security Rule – "establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity" [The Security Rule is located at 45 CFR Part 160 and Subparts A and C of Part 164] (HHS, 2017).

Subject Matter Experts – "a person with bona fide expert knowledge about what it takes to do a particular job" (U.S. Office of Personnel Management, n.d., para 1).

List of Acronyms

A – Addressable (Security Rule Implementation Specification)

AEHIS - Association for Executives in Healthcare Information Security

AMC - Academic Medical Center

ANSI – American National Standards Institute

BA – Business Associate (HIPAA Classification)

CAE – Centers of Academic Excellence (National Security Agency)

CC – Characteristics and Capacities (Independent Variable)

CE – Covered Entity (HIPAA Classification)

C.F.R - Code of Federal Regulations

CHIME - College of Healthcare Information Management Executives

CHWG – Cyber Healthcare Working Group

CISSP - Certified Information Systems Security Professional

CMMS - Centers for Medicare and Medicaid Services

DHS – U.S. Department of Homeland Security

DoD – U.S. Department of Homeland Security

DT – Deterrence Factors (Independent Variable)

DV – Dependent Variable

ePHI - electronic protected health information

EHR – electronic health record

EMR – Electronic Medical Records

EUT – Expected Utility Theory

GDT – General Deterrence Theory

GRC – Governance, Risk and Compliance

H1-H4 – Hypotheses (H1, H2, H3, and H4)

HCCA - Health Care Compliance Association

HHS - United States Department of Health and Human Services

HIMSS - Healthcare Information Management Systems Society

HIoT - Healthcare Internet of Things Executive Security Summit

HIPAA - Health Insurance Portability and Accountability Act

IAPP – International Association of Privacy Professionals

IBM - International Business Machines

IRB - Institutional Review Board

IA – Information Assurance

IP – Internet Protocol

IS - Information System

IT – Information Technology

IV – Independent Variable

MIC3 – Michigan Cyber Civilians Corp

MLR – Multiple Linear Regression

MT – Motive (Independent Variable)

NIST – National Institute of Standards and Technology

NSA – National Security Agency

NSU – Nova Southeastern University

OCR - Office for Civil Rights

OPM - U.S. Office of Personnel Management

PC1 – Perceived Likelihood of Security Rule Compliance (Dependent Variable)

R – Required (Security Rule Implementation Specification)

RR – Regulator Respect (Independent Variable)

RQ - Research Question

SEC – U.S. Securities and Exchange Commission

SIRA - Society of Information Risk Analysts

SME - Subject Matter Expert

SPSS - Statistical Package for Social Sciences

SRA- Security Risk Assessment

SRC - SRCS – Security Rule Compliance

SRCS – Security Rule Compliance Survey

SR – Security Rule

VIF – Variance Inflation Factor

Summary

SR compliance enforcement actions were initiated in 2005, yet, CEs & BAs remain challenged to comply with the SR even today. SR compliance research is limited, as compliance research is challenging to design, measure, and implement (Parker & Nielsen, 2010). The absence of the ability to directly measure SR compliance creates challenges for CEs &BAs as well as researchers (McLeod & Dolezel, 2018). This research study sought to identify, assess, and understand the difficulties CEs & BAs face with compliance to the SR regulatory strategy. Sittig et al. (2017), like many others since the SR's inception, have called for everyone involved in the healthcare industry to step-up and adopt a shared responsibility for the security of ePHI and create measures for CEs & BAs to be successful in HIPAA compliance. This research study helped to address this need by developing a unique conceptual model, one that integrated a holistic theoretical design and approach. This research study was designed to assess empirically (a) motives,

(b) characteristics and capacities, (c) regulator respect, and (d) deterrence factors that affect the perceived likelihood of complying with the HIPAA SR.

Chapter 2

Review of the Literature

Overview

A literature review to synthesize previous research regarding HIPAA compliance, regulatory strategy, SR compliance, and regulatory compliance was completed by electronic database searches. Keywords, backward searches, and review of existing literature were conducted to narrow down relevant research studies (Levy & Ellis, 2006). This literature review provided an understanding of the current research activities and body of knowledge in support this study's activities and research problem of Why CEs & BAs remain challenged to comply with the HIPAA SR regulatory strategy (Holtzman, 2017; Litten, 2017; Mohammed et al., 2015; Rodriguez, 2013; Sanches, 2017; U.S. Department of Health and Human Services Office for Civil Rights (OCR)., 2018d).

The literature review focused on the definition of the SR, its three core safeguard categories, as well as a brief overview of SR sanctions and non-compliance implications. Additionally, previous research studies were scrutinized to develop an understanding of HIPAA SR compliance, compliance perceptions, previously reported theories, and methodologies, as well as remaining knowledge gaps. The construct section of the literature review provides a focused synthesis of previous research, which directly supported, and aided in developing this research study's constructs of :(a) motive, (b) characteristics and capacities, (c) regulator relationship, (d) deterrence factors, and (e) the perceived likelihood of complying with the HIPAA SR.

What is the Security Rule?

The HIPAA Security Rule (SR) seeks to "protect an individual's *electronic* [emphasis added] personal health information that is created, received, used, or maintained" by a CE or BA (Alder, 2017, p. 18). Table 1 displays the three main SR compliance categories or safeguard requirements. The SR safeguard categories are administrative, physical, and technical. These major categories were created to identify appropriate security safeguards that would help CEs & BAs achieve compliance with the SR. Within each safeguard category, several standards are defined. These standards each have a correlated *Code of Federal Regulation* section number designation, derived from the 45 *C.F.R.* § 164 Subpart C of the official federal regulation. Additionally, and more importantly, Implementation Specifications for SR standards are also included.

The Implementation Specifications are categorized as either "Required" (R) or "Addressable" (A) (U.S. Department of Health & Human Services. Office for Civil Rights (OCR), 2010). For Required specifications, CE's & BA's must implement the specifications as defined in the SR. For addressable specifications, CEs & BAs must assess and document whether the implementation of the specification is reasonable and appropriate for their environment and the extent to which it is appropriate for the protection of ePHI data (OCR 2010).

Table 1

HIPAA Security Rule Standards Matrix (OCR, 2010)

Administrative Safeguards

Standards	**Sections**	**Implementation Specifications (R)=Required, (A)=Addressable**
Security Management Process	164.308(a)(1)	Risk Analysis (R) Risk Management (R) Sanction Policy (R) Information System Activity Review (R)
Assigned Security Responsibility	164.308(a)(2)	(R)
Workforce Security	164.308(a)(3)	Authorization and Supervision (A) Workforce Clearance Procedure Termination Procedures (A)
Information Access Management	164.308(a)(4)	Isolating Healthcare Clearinghouse Function (R) Access Authorization (A) Access Establishment and Modification (A)
Security Awareness and Training	164.308(a)(5)	Security Reminders (A) Protection from Malicious Software (A) Log-in Monitoring (A) Password Management (A)
Security Incident Procedures	164.308(a)(6)	Response and Reporting (R)
Contingency Plan	164.308(a)(7)	Data Backup Plan (R) Disaster Recovery Plan (R) Emergency Mode Operation Plan (R) Testing and Revision Procedure (A) Applications and Data Criticality Analysis (A)
Evaluation	164.308(a)(8)	(R)
Business Associate Contracts and Other Arrangement	164.308(b)(1)	Written Contract or Other Arrangements (R)

Table 1 (continued)

HIPAA Security Rule Standards Matrix (U.S. Department of Health & Human Services. Office for Civil Rights (OCR), 2010)

Physical Safeguards

Standards	**Sections**	**Implementation Specifications (R)=Required, (A)=Addressable**
Facility Access Controls	164.310(a)(1)	Contingency Operations (A) Facility Security Plan (A) Access Control and Validation Procedures (A) Maintenance Records (A)
Workstation Use	164.310(b)	(R)
Workstation Security	164.310(c)	(R)
Device and Media Controls	164.310(d)(1)	Disposal (R) Media Re-use (R) Accountability (A) Data Backup and Storage (A)

Technical Safeguards (see §164.312)

Standards	**Sections**	**Implementation Specifications (R)=Required, (A)=Addressable**
Access Control	164.312(a)(1)	Unique User Identification (R) Emergency Access Procedure (R) Automatic Logoff (A) Encryption and Decryption (A)
Audit Controls	164.312(b)	(R)
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information (A)
Person or Entity Authentication	164.312(d)	(R)
Transmission Security	164.312(e)(1)	Integrity Controls (A) Encryption (A)

In Table 1, under the Security Management Process, the first required implementation specification is risk analysis. The SR risk analysis requirement states that CEs & BAs must, “Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of *electronic* [emphasis added] protected health information held by the covered entity" (45 *C.F.R. §* 164.308 (A), 2011 p. 852). Moreover, HIPAA's SR requires the implementation of "reasonable and appropriate" security measures (HHS 2003, p. 8334). This scope of compliance requires CEs & BAs to consider "all relevant losses that would be expected if the security measures were not in place" (HHS, 2003, p. 8347). These universal SR standards and statements encompass broad mandates, which could leave CEs & BAs challenged to interpret what precisely is "accurate and thorough." This ambiguity impacts their ability to comply with the SR (Beaver, 2018). Some governmental agencies have tried to help clarify the wording of the regulatory strategy and provided more explicit SR guidelines for CEs & BAs.

The National Institute of Standards and Technology (NIST) is one agency that is helping clarify the safeguards of the SR. NIST offers resources, tools, and outlines methodologies to aid CEs & BAs in understanding SR mandates. For example, NIST Special Publication 800-30 provided insights and methodologies for security risk assessment (SRA), management, and SR compliance (G. Stoneburner, Goguen, & Feringa, 2002; J. A. Gold & Trudell, 2015; U.S. Department of Health & Human Services, 2010). Hash et al. (n.d.) provided a matrixed crosswalk report that affords CEs & BAs the ability to find related NIST guidance for all three main SR compliance safeguard areas (Drolet, Marwaha, Hyatt, Blazar, & Lifchez, 2017). However, compliance is difficult, especially when dealing with electronic data. Even though previous clarification efforts have been provided, they may only help to complicate the labyrinth of SR standards, mandates, and implementation specifications even further

(Beaver, 2018; McMillan, 2015). Moreover, smaller CEs & BAs may not have the internal resources or the financial ability to hire external expertise to interpret the complex nature of SR mandates. Nevertheless, if CEs & BAs do not comply with the regulatory strategy, they may face OCR investigations, severe penalties, fines, and potential criminal charges for non-compliance (Cogan, 2005; Sanches, 2017).

Compliance Implications

Although the U.S. Department of Health and Human Services Office for Civil Rights (OCR) prefers to settle violations using nonpunitive measures (Redspin, 2016), non-compliance can be costly (HIPAA Journal, 2017; Redspin, 2016). Noncompliance with HIPAA and SR puts CEs & BAs at significant risk of monetary loss through sanctions, fines, and civil monetary penalties imposed from breach investigations and regulatory audits. Healthcare Information Management Systems Society (HIMSS) (2013, 2014, 2015, 2016, 2017 2018) reports have stated, year after year, that although there have been encouraging efforts toward the protection and securing of ePHI data, not all organizations are upholding their compliance responsibilities. In some instances, ePHI security has not even been a priority (American National Standards Institute (ANSI), 2012; CMMS Medicaid Services, 2009). In 2010, research by Appari, Johnson, and Appari (2010) stated that the low levels of compliance should garner attention from the research community to examine HIPAA compliance-related issues on several fronts. Nine years later, sadly, the SR compliance landscape has changed very little (Sanches, 2017).

Chen and Benusa (2017a) and HIMSS (2018) research and industry reports have found that regulatory compliance with patient information security and privacy has become one of the most significant challenges in the healthcare industry. Demartine et al. (2017) predicted that healthcare breaches would become an everyday occurrence. As a result, SR compliance research is needed and is critical toward understanding why compliance with the SR regulatory strategy is still a challenge for CEs & BAs.

Current State of Research

The official regulations of the SR were published in 2003 (HHS, 2010)(45 *C.F.R.* § 164, (2011). Despite being published over a decade ago, very little academic and industry research has been conducted on the SR (Martin et al., 2015). Most existing research and literature focus on overall privacy compliance to HIPAA, but not SR compliance. The overall HIPAA compliance approach is understandable, as the SR is integrated into the HIPAA regulation strategy. However, the SR itself is unique, having 22 standards and more than 50 implementation specifications, specifically aimed at dealing with ePHI data. Because the SR regulatory strategy contains many different standards and special compliance implementation considerations, research specific to the SR is critical (Beaver, 2018).

SR compliance research often deals with highly sensitive information and could expose incriminating results (Drahos, 2017a; Losoncz, 2017). Research assessing compliance to a regulatory strategy is a sensitive topic, and it can be challenging to get an actual compliance posture data from organizations; CEs & BAs are hesitant to air any dirty laundry (Parker, 1999). It is only operationally and financially prudent for CEs & BAs not to air their dirty laundry. However, in a climate where compliance with the SR regulatory strategy is stagnated, and with cyber-attacks on healthcare increasing daily, additional research is needed to help better protect ePHI (HIMSS, 2018). As such, this research study was designed to address the scarcity of data in this area.

HIPAA compliance and business regulatory compliance research cover several different industry sectors; including, medical, business, and academic. There are HIPAA compliance studies conducted in Academic Medical Centers (AMCs) like that of Brady (2010) and others where students and faculty of academia are the participants of the research study (X. Chen et al., 2018; Gaia et al., 2018). There are even a few studies where a broad cross-section of different industry types were selected (Nielsen & Parker, 2012; Sohrabi Safa, Von Solms, & Furnell, 2016).

Sohrabi Safa, Von Solms, and Furnell (2016) research collected data from the business, information technology (IT), education, and government-industry types regarding information security policy compliance. Sohrabi Safa, Von Solms, and Furnell (2016) reported that personal norms and information security involvement increase user’s awareness and propensity to comply. However, the study was based on a cross-section of Malaysian industries and based its information on security policies already in place. Furthermore, that study focused on user attitude and awareness of the policy, not the organization’s compliance posture to a regulatory strategy.

A robust (non-HIPAA) regulatory compliance study was conducted by Nielsen and Parker (2012) in the Australian business sector. The study included 999 participants, which represented a broad cross-section of the Australian industry. The participants were all targets of the Australian Competition and Consumer Commission regulatory enforcement activity in previous years. Nielsen and Parker (2012) investigated the distinct business motives for compliance among three dimensions: economic motives, social motives, and normative motives. They suspected that firms use a combination of these motives when making compliance decisions. To that end, their data supported the idea that firms hold a pluralistic mix of motives in regards to compliance. Nielsen and Parker (2012) suggested that their conceptual model should be used across other types of industries to help better understand compliance. With the permission of Nielsen and Parker (2012), this study sought to understand healthcare SR compliance better. Previous studies involving non-HIPAA industry types have proven useful, but research into the medical industry’s SR remains limited.

A substantial gap in HIPAA SR research exists, especially for CEs & BAs operating within the medical industry of the U.S. Previous research is limited to single case studies, pure academic studies, or have questionable generalizability due to low sample sizes (Burch & Heinrich, 2016). For example, a case study conducted by J. Chen and Benusa (2017) included a single optometry service provider and its challenges to comply with the HIPAA regulatory strategy. In this study, the focus was on a smaller healthcare provider's intention to comply with the HIPAA regulatory strategy. J. Chen and Benusa (2017) identified constructs, such as breach cost, compliance cost, financial resources, and expertise as factors that impact a provider's intentions to comply. This study, although it included just a single business is more pragmatic than academic research in that it offered operational risk mitigation solutions, as opposed to trying to assess constructs empirically.

Another case study by Reis (2012) utilized an academic medical center and seven semi-structured interviews to examine the intersection of IT security frameworks and project management. This study offered a unique look at the challenges of building

HIPAA compliance, but into that of IT projects and IT security frameworks. Cannoy and Salam (2010) leveraged a case study approach and interviewed eight radiology professionals to reach their research conclusions. Their research purported a lack of well-developed information security frameworks that understand compliance factors. Cannoy and Salam (2010), posited a framework that accounts for (a) external factors, (b) beliefs, and (c) attitudes. Cannoy and Salam (2010) concluded that the factors, as mentioned earlier, impact the intention to comply with an information assurance policy. Their conclusion stated that employees with a high propensity for compliance beliefs, along with higher-level management intervention and support, positively impacted an organization's commitment and level of compliance to the HIPAA regulatory strategy. Although this study was carried out in the U.S. healthcare industry, the authors acknowledged the difficulty of generalizing their findings, and recommended further research studies.

Liginlal, Sim, Khansa, and Fearn (2012) investigated the HIPAA privacy rule based on interviews from 15 privacy officers employed with major healthcare organizations in the U.S. Liginlal, Sim, Khansa, and Fearn (2012) focused on the HIPAA privacy rule and is one of the few U.S based academic research studies that have assessed the medical industry. Liginlal, Sim, Khansa, and Fearn (2012) reported that human error is the leading cause of privacy breaches. Their research created a framework for compliance, as it related to human error, and provided strategies to reduce and identify human errors. Their results showed that organizations have difficulty complying, especially when errors are systemic, knowledge-based mistakes, or are committed by clinical staff. Human error contributes to noncompliance with the HIPAA regulatory strategy and is an ongoing challenge. However, their research did not provide how an organization approaches compliance to the regulatory strategy. Similar to the majority of previous research studies, the authors stated that the generalizability and external validity of their model was limited due to the small sample size.

The sparsity of HIPAA regulatory strategy research that is robust and generalizable, one which focuses on the organizational challenges to the regulatory strategy, appeared to be a persistent knowledge gap. Additionally, the conspicuous absence in research of this nature may once again hint at the level of difficulty that compliance-focused researchers face when attempting to assess the medical industry in U.S. based CEs & BAs. As a result, and perhaps in the absence of being able to engage with the U.S. medical industry directly, some researchers have utilized the publicly available Dorenfest Institute healthcare databases to provide the necessary data for their research.

The Dorenfest Institute is a research division of HIMSS (HIMSS Analytics, 2019). The Dorenfest Institute helps meet the researcher's demand for U.S. based healthcare and healthcare information technology data. These datasets currently range in years covering the 2003-2015 period and provide demographic and IT data from 40,000 healthcare and healthcare information technology facilities (HIMSS Analytics, 2019). Although somewhat dated, research conducted by Appari et al., (2006) and Appari, Anthony, and Johnson (2009) as well as Anthony et al., (2014) focused on HIPAA compliance in hospitals using the Dorenfest Institute 2003 dataset.

Appari et al. (2006) research investigated which hospitals in the U.S. are complying with HIPAA. Focusing on the hospital characteristics of; (a) IT leader (based on technology used); (b) Profit status- nonprofit, for-profit; (c) academic status; (d) hospital size and (e) Electronic Medical Record (EMR) system, they purported the creation of the first empirical evidence of a hospitals propensity to be compliant with HIPAA. By leveraging the HIMSS dataset and the American Hospital Association's listing of the 100 most wired hospitals, they created a custom dataset for their research. Although this study has many insights, what becomes foundationally troubling is that in the HIMSS raw dataset, the hospitals self-reported their perceived level of compliance to HIPAA. This self-reported perceived level of compliance data variable was on an ordinal scale of <50%, 50-75%, and 100% compliance. Whereby the researchers then transformed this into a dichotomous value of 1 being 100% compliance and 0 otherwise. This approach is concerning for a couple of reasons, first of all, compliance to the HIPAA is self-reported and not empirically assessed or validated by some other means and secondly by dichotomizing the variable, some results may appear to show compliance, when that may not indeed be the case. As a side note, it appears that after 2003, the HIMSS data sets no longer include this self-reporting HIPAA compliance variable.

Appari et al. (2006) research is substantially dated and conducted during a time when enforcement to HIPAA's SR was beginning. Although HIPAA enforcement started in 2005, it did not gain momentum until after 2009 (Asmonga et al., 2004). There does appear to be current academic research studies covering healthcare compliance, although it is of foreign origin.

Kuo et al. (2018) research collected data from a large (1300 beds) Taiwanese medical center. Utilized in the study was a convenience sampling of 2800 healthcare professionals and 100 healthcare administrators who were authorized to access EMR data. This survey-based research study investigated possible antecedents that influence hospital employee’s continuance of compliance with the privacy policy of EMR data. Specifically, the research focused on the motivational and habitual perspectives and found that self-efficacy, perceived usefulness, and facilitating conditions significantly predicted an employee’s compliance habit formation. Overall the study found that habit is a critical element that can positively predict an employee’s intention of adherence to the privacy policies of the hospital.

In another recent international academic study, Ahmed, Hepu, Booi, and Xiaojuan (2017) investigated how institutional pressures influence information security compliance. Their study was based on a cross-section of industry types operating in the public sector of Oman. The research was centered on compliance with organization information security policies and not governmental regulatory compliance strategy. Furthermore, only 12% or 35 out of 294 participants were in the healthcare industry. The results showed that coercive pressures, normative pressures, and mimetic pressures positively influence information security compliance in Oman organizations.

Al-Mukahal and Alshare (2015) research and model were tested from a cross-section of industries in Qatari. Their study investigated factors of trust, compliance implementation impact, IS policy clarity, and its impacts on information security policy violations. Although the results showed that all these factors are significant in predicting the number of information security policy violations, the authors admit there may be limited generalizability due to the model being tested in a developing country. Although there is knowledge to be gleaned from academic research studies based on international populations and industries, it may be limited toward understanding challenges that exist with U.S. based regulatory strategies like that of HIPAA and the SR.

As a result, with the limited academic U.S. based HIPAA SR research, and the continual challenges that CEs & BAs are facing toward complying with the HIPAA SR regulatory strategy, there appeared to be a compelling need for additional academic research. The said need is further substantiated by the fact that most of the existing research that appeared to deal strictly with HIPAA SR, actually investigate overall HIPAA privacy rule compliance or compliance to overarching information security rules (Brady, 2010; Kolkowska & Dhillon, 2013). Therefore, this research study addressed the need to empirically investigate HIPAA SR compliance issues in CEs & BAs operating in the U.S.

Theoretical Frameworks

Past research studies in HIPAA compliance, information security policy compliance, and regulatory compliance have leveraged various theoretical frameworks toward HIPAA compliance assessment and investigations. Theoretical frameworks can provide a basis for generating hypotheses about what the data may potentially reveal (Creswell & Guetterman, 2019). In some instances, researchers seek to find support for the theory used or refute a particular theory (Leedy, 2016). Table 2 illustrates the various theoretical frameworks related to the research studies in this literature review. Table 2 provides the theory the research used, who conducted the study, sample size, and instrument utilized for the literature review.

Table 2

Summary of related literature

Theory Used	Study Conducted by	Sample	Instrument
Agile Theory	Reis, D. W. (2012)	1 - AMC	Interviews
Compliance theory	Chen, J., & Benusa, A. (2017)	1 Ophthalmology and Optometry practice	Case study
Compliance Theory	Appari, A., Anthony, D. L., & Johnson, M. E. (2006)	1342 hospitals with > 100 beds	HIMSS Dorenfest data
Expected Utility Theory	Gaia, J., Wang, X., Basile, J., Sanders, G. L., & Murray, D. (2018)	574 IT undergraduate students	Survey
General Deterrence Theory	Chen, X., Wu, D., Chen, L., & Teng, J. K. L. (2018)	231 employees - U.S. based university	Survey
General Deterrence Theory Neutralization theory Theory of Planned Behavior	Al-Mukahal, H. M., & Alshare, K. (2015)	234- Qatari Orgs	Survey
Institutional Theory	Ahmed, A., Hepu, D., Booi, K., & Xiaojuan, Z. (2017)	294- Oman Orgs	Survey
Institutional theory	Angst, C. M., Block, E. S., D 'Arcy, J., & Kelley, K. (2017)	HIMSS Dorenfest data	HIMSS database
Institutional Theory	Appari, A., Anthony, D. L., & Johnson, M. E. (2009)	1564- U.S. based hospitals	HIMSS database
Motivational Theory	Nielsen, V., & Parker, C. (2012)	999 -Australian Orgs	Survey

Table 2

Summary of related literature (continued)

Protection Motivation Theory	Vance, A., Siponen, M., & Pahnila, S. (2012)	54	Scenario vignette
Psychological Resource Theory	Zhang, N., & Zhang, N. (2018)	224-Global Insurance Co.	Survey method
Reasoned Action Theory	Cannoy, S. D., & Salam, A. F. (2010)	8 - Radiology Professionals	Interviews
Reasoned Action Theory	Brady, J. W. (2010)	76- AMCs	*Survey*
Self-determination Theory	Kuo, K. M., Chen, Y. C., Talley, P. C., & Huang, C. H. (2018)	312 - Taiwan healthcare	Survey
Self-determination Theory	Alzahrani, A., Johnson, C., & Altamimi, S. (2018)	407- Fortune 600 Saudi Orgs	Survey
Social Bond Theory Investment Theory	Sohrabi Safa, N., Von Solms, R., & Furnell, S. (2016)	462- Malaysia Orgs	Survey
Social Influence Theory Informational Influence Theory	Barlow, J. B., Dennis, A. R., Warkentin, M., & Ormond, D. (2018)	200- Qualtrics provided	Survey
Theory of Planned Behavior	Bulgurcu, B., Cavusoglu, H., & Izak, B. (2010)	464- research company provided	Survey

Table 2 highlights the diversity in theoretical frameworks applied to HIPAA compliance, information security policy compliance, and regulatory compliance research. Furthermore, almost all the research identified in Table 2 posited a single theoretical approach toward explaining compliance behaviors, intentions, and perceptions. Moreover, there are theoretical frameworks that appeared to be more common to use, as indicated by the repetition in Table 2.

Single theoretical approaches are troubling because there is disagreement in the research community about the efficacy of compliance research that uses one theoretical lens to investigate such highly complex topics like that of behaviors, intentions, and perceptions toward compliance with HIPAA or any regulatory strategy (Losoncz, 2017). An in-depth literature review has identified that investigating healthcare CEs & BAs responses to HIPAA SR regulatory strategy with a multi-lensed theoretical framework and approach appears to be a prudent approach and an active area for development (Parker & Nielsen, 2011). This research study addressed this knowledge gap as it developed a holistic conceptual model based on multiple theoretical approaches toward solving a very challenging issue; why CEs & BAs remain challenged to comply with the HIPAA SR regulatory strategy

Constructs

Motive. Alzahrani, Johnson, and Altamimi (2018); Bulgurcu, Cavusoglu, and Benbasat (2010); Kuo, Chen, Talley, and Huang (2018); Nielsen and Parker (2012); Parker and Nielsen (2017); Treekrutpant (2017) and Vance, Siponen, and Pahnila (2012) research viewed motive as a significant determinant in compliance behaviors as well as one's intention to comply. Alzahrani, Johnson, and Altamimi (2018) leveraged self-determination theory to discover that intrinsic motivation significantly impacted behavioral intentions toward organizational compliance. Bulgurcu, Cavusoglu, and Izak (2010) empirical research leveraged the rational choice theory to discover an employee’s intention to comply with organizational IS policies are significantly influenced by one's attitude, normative beliefs, and self-efficacy. However, they note that future research should investigate and integrate the impact of deterrence and subjective norms that may impact one's intention to comply since their underlying conceptual model did not account for these factors. Treekrutpant (2017) research in the airline regulatory industry-linked motivation to self-efficacy and Vance, Siponen, and Pahnila (2012) stated that self-efficacy had a positive impact on employee intentions to comply with IS policies. Moreover, Kuo et al. (2018) research in a large Taiwanese medical center empirically validated that motivation (intrinsic and extrinsic) significantly predicted compliance intention. However, Kuo et al. (2018) study focused on one Taiwanese medical center, thus impacting generalizability, yet opening a door for future researchers to include more healthcare organizations.

Parker and Nielsen (2011) stated that most compliance research generally uses a classical deterrence theory approach in explaining or identifying why individuals are motivated to comply with regulations. Whereas, motivation is more complicated, leading Parker and Nielsen (2011) to extend what accounts for motivation in compliance research to that of a pluralistic definition; economic (material), social, and normative motives. Drawing on motivational theory, Nielsen and Parker (2012) purported that compliance motives are, therefore, not an either/or situation but are different variations and combinations of all three. Research data from 999 of Australia’s largest companies validated that all the firms held a variated mix of economic, social, and normative motives toward compliance. Furthermore, Nielsen and Parker (2012) suggested that future researchers should leverage this mixed motive definition into a broader variety of businesses, types, sizes, and even countries. Additionally, Parker & Nielsen (2011) recommended that future researchers look at the connections and combinations of motives to comply along with other factors (internal and external) that influence or explain compliance behaviors or intentions. Therefore, this research adopted the pluralistic definition of motive (economic, social, and normative) purported by Nielsen and Parker (2012) as an independent variable, for the insight the pluralistic definition may provide in this research endeavor.

Characteristics and capacities. If an organization wants to comply with regulatory strategies and compliance demands, it must have the capacity to do so (Parker & Nielsen, 2011). Angst et al. (2017), Brady (2010) and J. Chen and Benusa (2017), as well as Nielsen and Parker (2012) and Parker and Nielsen (2017) research inquiries, have determined that an organization's characteristics and capacities are significant determinants in compliance behaviors as well as an organization's intention to comply. Angst et al. (2017) research regarding cyber breaches and hospital information technology (IT) security investment efficacy investigated several characteristics and capacities in hospitals and their impact on IT security behaviors. Their model leveraged several characteristics and capacities of healthcare to predict if the organization was a substantive or symbolic adopter of information technology (IT) security practices. The latent class variables of health system size, hospital age, profit type, and an entrepreneurial mindset are characteristics and capacities served as predictors for IT security adoption practices.

Angst et al. (2017) noted that the SR only defines a baseline level of security controls. The SR has no specific requirements for the types of technology to implement, meaning that organizations have a great deal of discretion and thus may find it nearly impossible to assess how well they are fulfilling their legal compliance requirements. J. Chen and Benusa (2017) investigated challenges for small healthcare providers to comply with or intentions to comply with the HIPAA mandates. J. Chen and Benusa (2017) single case study indicated that the organizational characteristics and overall lack of security, as well as limited IT security knowledge capacity, are typical in smaller entities. Furthermore, smaller healthcare entity's financial capacity to afford the cost of compliance is equally challenging, if non-existent.

Brady (2010) researched SR compliance in academic medical centers. Brady (2010) and Johnston and Warkentin (2008) have identified the organizational characteristic of management support as being significant and a valid predictor for HIPAA SR compliance in academic medical centers as well as healthcare facilities. Since there is no direct way to measure if an organization is compliant to the SR. Brady (2010) model identified security behaviors and security effectiveness as characteristics to predict the intention to comply with the HIPAA SR compliance regulatory strategy. Johnston and Warkentin (2008) leveraged organizational status (profit or nonprofit), healthcare types, and used the constructs of self-efficacy, perceived organizational support, and behavioral intent as antecedents to predict compliance behaviors. However, Brady (2010) research is limited to academic medical centers and Johnston, and Warkentin (2008) was limited to only administrative staff members. Thus, once again severely limiting the generalizability of these research studies.

Parker and Nielsen (2017) purported the motivation to comply, and the level of organizational compliance may be based on an organization’s characteristics and capacities, i.e., financial, technical, knowledge, and management systems and support. Parker and Nielsen (2006) extensive research in Australian trade practices and paper mill regulatory compliance affirms that the organizational characteristic and capacities mentioned are factors that deserve investigation when investigation as well as attempting to explain compliance behaviors or the intent to comply with regulatory strategy (Parker & Nielsen, 2006, 2011). Therefore, this research utilized characteristics and capacities as an independent variable to assess the effect these factors have on U.S. based healthcare CEs & BAs perceived likelihood of complying with HIPAA SR.

Regulator respect. Parker and Nielsen (2010, 2011, 2017), research inquiries, have determined that regulator respect is a significant determinant in compliance perceptions and an organization's intentions to comply. Parker and Nielsen (2017) purported that regulator respect may influence all other dimensions of compliance within a regulatory strategy. Awareness and perception of the regulator’s actions and enforcement strategies can only make an impact on compliance posture if the organization perceives fairness in its regulatory dealings (Parker & Nielsen, 2017). In the absence of regulator respect, organizations often symbolically adopt or go through the compliance motions without permanently impacting their compliance behaviors or posture (Angst et al., 2017; Parker & Nielsen, 2010, 2017). Thus, it appears that accounting for the organizational relationship perception of the regulatory agency responsible for enforcement and supporting them to achieve compliance is a factor that affects compliance or the intent to comply. Therefore, this research utilized regulator respect as an independent variable to assess the effect this factor has on the U.S. based CEs & BAs perceived likelihood of complying with the HIPAA SR.

Deterrence factors. X. Chen, Wu, Chen, and Teng (2018), Gaia, Wang, Basile, Sanders, and Murray (2018) and Gunningham (2010), as well as Parker & Nielsen (2017) and Weistroffer (2016) research inquiries, have determined that deterrence factors are significant determinants in an organization’s perceptions of and intentions to comply with regulatory strategies. Punitive or coercive sanctions to get regulatees to conform to compliance mandates appear deeply interwoven into the fabric of regulatory enforcement strategy (Weistroffer, 2016). Grounded in criminology, the general deterrence theory (GDT) purports that swift and severe sanctions deter individuals from violating laws or rules (Gunningham, 2010). However, the perceptions of the risk of being caught and the perceived legal severity or ramifications may play a more significant role in compliance behaviors and intentions to comply (Gunningham, 2010). X. Chen et al. (2018) stated that previous research leveraging GDT and sanctions to deter compliance intention had produced different and mixed results. Furthermore, their research results showed that the perceived sanctions and perceived sanction severity were variables that impacted compliance intention. As insightful as X. Chen et al. (2018) findings are, they are limited to only one higher educational institution and state the research findings generalizability is questionable. Gaia et al. (2018) research of factors impacting HIPAA non-compliant behavior leveraged the expected utility theory (EUT). Gaia et al. (2018) identified the risk aversion level and the perception of getting caught (reporting, inspection, and detection) as factors that influence HIPAA compliance perceptions and behaviors on the intention to comply. However, their research focused on one academic institution, making generalizability questionable. Moreover, Gaia et al. (2018) suggested that future research should be conducted in healthcare organizations to test their model and findings better. Parker and Nielsen (2017) stated that the perception of risk has more of an impact on regulatees than the actual deterrence risk. Moreover, an organization’s perception that non-compliance will not be detected or reported and perceived risk of a regulatory inspection may be factors that influence compliance levels more significantly than financial sanctions. Therefore, this research utilized deterrence factors as an independent variable to assess the effect this factor has on U.S. based CEs & BAs perceived likelihood of complying with the HIPAA SR.

The IVs of motive, characteristics and capacities, regulator respect, and deterrence factors developed for this research study and conceptual model were derived from and supported by past research and literature. Past research has shown conflicting results, lack of generalizability, and numerous single lensed theoretical approaches toward explaining compliance, perceptions toward compliance, and intentions to comply. The complexity of compliance and regulatory strategy research forces one to traverse and integrate concepts from a variety of academic disciplines as well as the assimilation of various theoretical frameworks in developing a holistic research model and approach. However, the primary challenge in the research of this nature is defining compliance.

Perceived likelihood of complying with HIPAA SR. Parker and Nielsen (2010) identified many challenges in empirical research regarding compliance. In research of this nature, compliance as a variable to be measured is understood to be developed from and related to external factors. The researcher determines the definition of and predefines compliance as a fixed variable that can be measured (Parker & Nielsen, 2011). The definition the researcher chooses must be in line with accepted definitions in the domain, and one that is reasonable as well as defendable (Parker & Nielsen, 2011). Thus, this research study investigated, measured, and attempted to explain the effects that the identified IVs of motive, characteristics and capacities, regulator respect and deterrence factors have on a DV; one defined as the perceived likelihood of complying with SR.

As previously mentioned, but worth reiterating here is that McLeod and Dolezel (2018) recognized that no standard method exists for CEs & BAs to measure or directly assess their compliance level to the SR. As a result, researchers like Brady (2010) and others have had to create and define unique constructs or combinations of constructs that serve as a proxies or surrogate DVs that define and measure SR compliance; in lieu of actually being able to directly measure SR compliance (Johnston & Warkentin, 2008; Parker & Nielsen, 2010). This research followed this pattern and the recommendations of Parker and Nielsen (2010) by using the IVs as determinates that ultimately predict a DV defined as the perceived likelihood of HIPAA SR compliance. This DV, as predefined, when empirically assessed in a holistic conceptual model that includes motives, characteristics, and capacity, regulator respect, as well as deterrence factors, may offer unique insight toward predicting the perceived likelihood of complying with the HIPAA SR regulatory strategy, thus SR compliance.

What is Known and What is Unknown

HIPAA compliance is a complicated, multifaceted, and challenging for CEs & BAs to understand, implement, and achieve (Vogenberg, 2019). There appeared to be limited HIPAA compliance academic research that is U.S. based while assessing the medical industry in a meaningful manner, i.e., industry type and population. Research specifically about the HIPAA compliance challenges to the SR appeared to be nonexistent, with most research focused on the overall HIPAA compliance mandates.

The academic research that does exist, most leveraged a single theoretical framework and small population samples on which their results were founded.

The review of the HIPAA academic literature gives the appearance that researchers have an information security mindset vs. an agnostic regulatory compliance approach. This initial mindset may curb or dampen regulatory compliance findings and perceptions due to the initial biases of approach (Leedy 2016). Furthermore, the populations and actual sample sizes whereby results were derived in the research reviewed appeared lacking in the ability to be generalizable due to the small population and participant industry types (academic vs. medical vs. business).

What is unknown is the level of willingness and sincerity in the responses of CEs & BAs when regulatory compliance research is conducted. As mentioned previously, research regarding compliance with regulatory mandates can be a very sensitive topic for organizations, one that can have substantial legal, governmental, and organizational implications (Haines, 2017). An additional unknown is the level of knowledge regarding HIPAA SR that the CEs & BAs have. As the literature review has shown, most academic compliance research blends the HIPAA privacy rules and security rules into one, whereas the SR strictly deals with ePHI.

Summary

Politics and the powers that be may often imply or present the notion that compliance with regulations can be quickly implemented (Parker & Nielsen, 2011). However, the historical lack of compliance to the SR proves this notion to be a fallacy. Past compliance research draws on a bewildering array of theories, constructs, and concepts from across a variety of disciplines (G. Robinson & Mcneill, 2012). The use of one theory, for example, institutional theory in a research approach, has its ability to identify specific influences of compliance or non-compliance perceptions, intentions, and behaviors (Ahmed et al., 2017). However, to adequately explain and understand compliance with regulatory rules, one has to extract many facets of organizational, individual, and even context-specific meanings that influence the perception and intentions of compliance (Parker & Nielsen, 2011). Even OCR appears to be looking for insight based on their recent public request for information regarding modifications to the HIPAA privacy and security rules. As a result, these research study findings appear to be very relevant and timely (OCR 2018c).

The general problem is that CEs & BAs remain challenged to comply with SR regulatory strategy. The academic literary landscape reveals that there is limited research devoted to CEs & BAs compliance with and adherence to the SR regulatory strategy. Furthermore, past literature studies have revealed that more compliance research is needed toward investigating the profoundly complex and often nuanced factors of (a) motive; (b) characteristics and capacity; (c) regulator respect; and (d) deterrence factors toward U.S. based healthcare CEs & BAs perceived likelihood of complying with HIPAA SR. Therefore, this research study developed and adopted a unique approach toward assessing the factors impacting SR compliance regulatory strategy. As a result, this research study offered an exclusive glimpse into the efficacy of the SR regulatory strategy and the related factors that have plagued HIPAA SR compliance in CEs & BAs, perhaps since the SR’s inception.

Chapter 3

Methodology

Overview of Research Methodology/Design

This study utilized a quantitative research design with a survey-based methodology. Figure 2 illustrates the three-phase research approach. Phase 1 developed and refined SRC survey questions and survey instrument with the help of subject matter experts (SMEs). Phase 2 performed a pilot study of SRC survey questions and instrument; that tested, refined, and added clarity to the SRC survey questions, as well as the survey instrument. Phase 2 officially launched and was distributed to the sampling population; healthcare CEs & BAs operating in the U.S. Phase 3 involved data screening, overall data analysis, and interpretation of results. Phase 3 addresses hypotheses H1-H4 as well as the research question and concluded with results write up and final reporting.

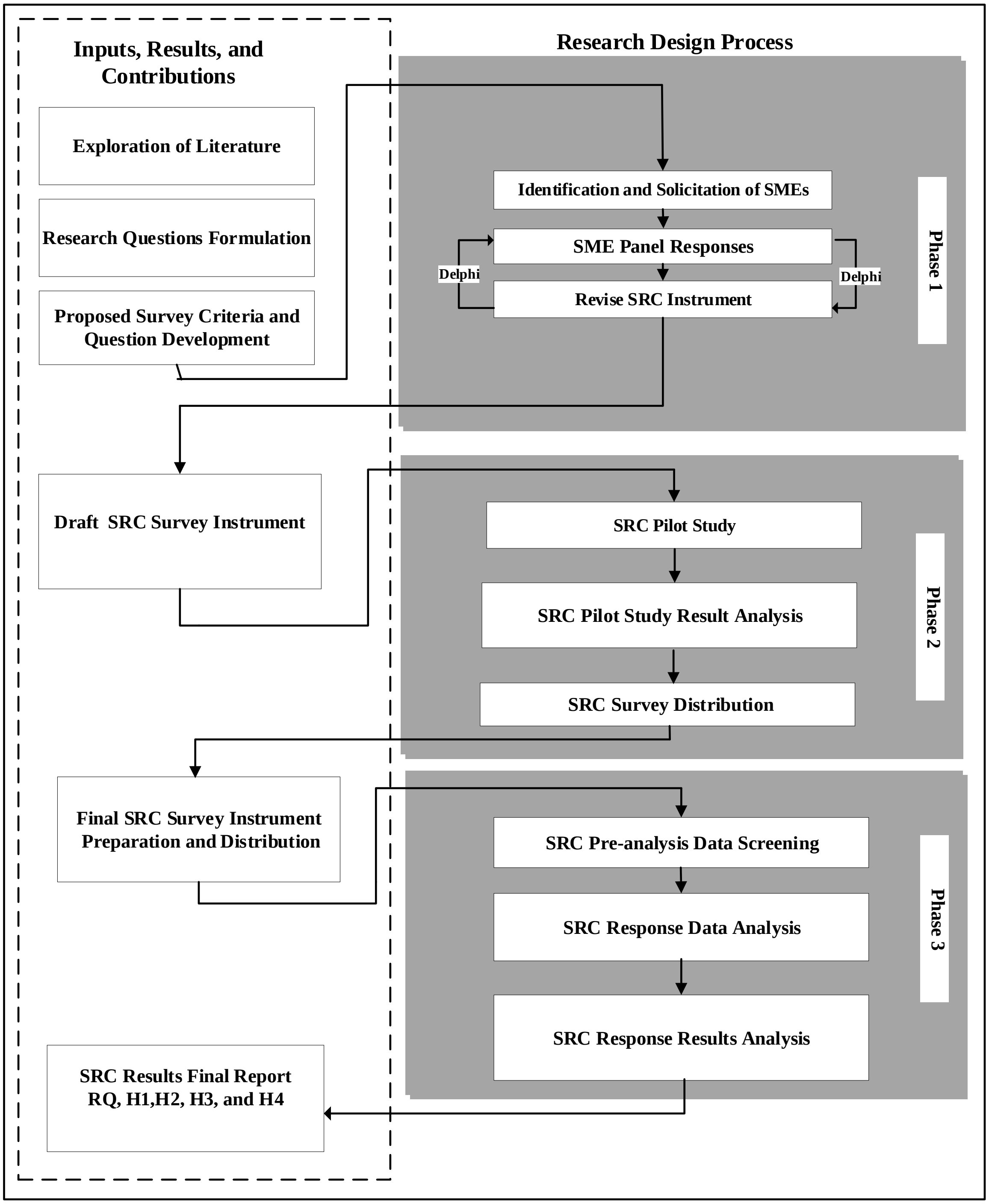

Inputs, Results, and Contributions
Exploration of Literature
Research Questions Formulation
Proposed Survey Criteria and Question Development
Draft SRC Survey Instrument
Final SRC Survey Instrument Preparation and Distribution
SRC Results Final Report RQ, H1,H2, H3, and H4
Research Design Process
Identification and Solicitation of SMEs
SME Panel Responses
Delphi
Delphi
Revise SRC Instrument
Phase 1
SRC Pilot Study
SRC Pilot Study Result Analysis
SRC Survey Distribution
Phase 2
SRC Pre-analysis Data Screening
SRC Response Data Analysis
SRC Response Results Analysis
Phase 3

Figure 2. Three Phase Research Design Diagram.

Population and Sample

The population of interest was healthcare CEs & BAs operating in the U.S. The SRC survey instrument provided participants the ability to select how their organization is best defined (CE or BA), as per HIPAA definitions and statutes, which was discussed in the background section of chapter one. This study identified specific healthcare industry types that CEs & BAs operate in to provide further analyses and understanding of the research question. Research for SR compliance by specific healthcare industry type remains an unfulfilled knowledge gap (Hoffman & Podgurski, 2006; Price Waterhouse Cooper, 2016).

When considering possible sampling strategies for the population of interest, such as random sampling, purposive sampling, systematic sampling, among others, a convenience sample was determined to be the most appropriate for this type of research study. A convenience sample is most appropriate because compliance with a regulatory strategy may be a very sensitive topic for organizations (Haines, 2017). Wu Suen, Huang, and Lee (2014) stated that convenience sampling is a type of non-probability or non-random sampling, where members of the sampled population meet specific practical criteria.

A large, reputable healthcare compliance software firm aided this research study. The owner of the firm participated as a project champion and served as a liaison for survey distribution. The relationship afforded this research study a unique opportunity to directly address over 3000 healthcare professionals. The project champion is part of several high-profile medical compliance working groups and professional healthcare organizations. In addition, the project champion has served as an expert witness in several HIPAA compliance investigations and court cases. The firm’s HIPAA compliance software has earned numerous endorsements from the American Medical Association, and other prolific healthcare and government organizations, not only for the software itself but also for the company's efforts in helping CEs & BAs understand and manage their HIPAA compliance needs.

After consulting with the project champion, it was estimated that the company had 400 clients and access to 2100 top-level healthcare executives, management, and information security professionals. All 2,500 clients and association members were invited to participate in the study. Moreover, previous survey response results from the project champion’s company had yielded a response rate of 16%. Due to this response rate, a sample size of 400 (2,500*0.16 = 400) was anticipated for this project. Healthcare and information security professionals included in the survey sampled population were:

- AEHIS - Association for Executives in Healthcare Information Security
- CHIME - College of Healthcare Information Management Executives
- HCCA - Health Care Compliance Association
- SIRA - Society of Information Risk Analysts

Phase 1

Phase 1 had several preliminary tasks to accomplish in order to develop the research study. A survey-based study was determined to be the most pragmatic research approach. The survey method was a suitable instrument to address the research question, as well as the goal of the proposed study (Creswell & Creswell, 2018b; Ruel, 2018). Creswell and Creswell (2018a) stated that the survey instrument provides quantitative data regarding trends, opinions, and attitudes about a sample population. Fowler (2014) reported that sometimes, the only way to ensure the researcher obtains the data they need is via a unique, purpose-built survey. Moreover, survey-based instruments have been a common practice among previous compliance researchers, as illustrated in the literature reviews found in Table 2 of the previous chapter.

A survey-based data collection strategy, concerning regulatory compliance perceptions and practices is common among researchers in this field because direct or indirect observation is impractical (Parker & Nielsen, 2010). The strength of a survey-based methodology lies in the fact that information provided by participants can often be highly representative or generalizable to the population of interest, provided proper sampling rigor, and techniques are followed (Ruel, 2018).

Figure 3 illustrates the tasks that are involved in Phase 1 of this research study. The primary research tasks were (a) exploration of literature, (b) research problem and question identification, and (c) development of research question(s) and creation of an initial SRC survey-based instrument. Phase 1 leveraged the identified constructs, as illustrated in Appendix F, Tables F1 - F5, toward the development of a final SR Compliance (SRC) survey. After identifying a research-worthy problem, formulating constructs to measure and assess the problem, the next step in Phase 1 was validation and further refinement of the SRC survey instrument, using subject matter experts (SMEs).

Figure 3 illustrates three distinct tasks during the SME stage of Phase 1: (a) identification and solicitation of SMEs, (b) initial survey solicitations, and (c) SMEs' responses, which were further analyzed. SME responses led to survey instrument refinement, via Delphi expert methodology. This research study used SME feedback to refine and clarify the survey questions and further developed the SRC instrument by employing the Delphi expert methodology.

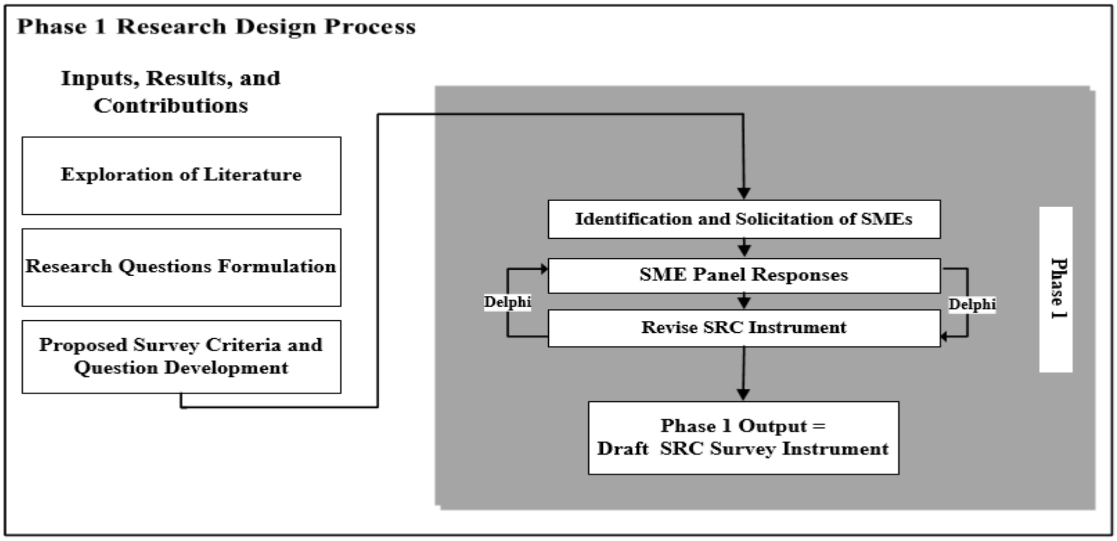

Phase 1 Research Design Process
Inputs, Results, and Contributions
Exploration of Literature
Research Questions Formulation
Proposed Survey Criteria and Question Development
Identification and Solicitation of SMEs
SME Panel Responses
Revise SRC Instrument
Delphi
Delphi
Phase 1
Phase 1 Output = Draft SRC Survey Instrument

Figure 3. Phase 1 Research Design and Process

Subject matter experts. The U.S. Office of Personnel Management (OPM). n.d.) defined an SME as “person with bona fide expert knowledge about what it takes to do a particular job” (para 1). Literature reviews conducted for this study revealed that using SMEs is a common research strategy (Brown, 1968; Trevelyan & Robinson, 2015). SMEs identified from a host of healthcare, and information security professions helped provide vital information for this research. By aligning experts from various fields, this project incorporated collective perspectives (Okoli & Pawlowski, 2004). In order to be considered for inclusion in this project, SMEs must have healthcare organization employment within the U.S. Additionally, SMEs with valid information security certifications, or other industry-related security or compliance accreditations, were highly sought.

SMEs identification. SMEs were solicited from industry contacts associated with this research project. According to the literature, there is no standard number of experts required for a Delphi panel. However, Okoli and Pawlowski (2004) stated that a practical Delphi expert panel size consists of approximately 10 to 18 members. The use of SMEs and the Delphi method is a common practice in IS research because it affords researchers the ability to capture the collective knowledge and expertise of professionals in the field (Ramim & Lichvar, 2014).

Ramim and Lichvar (2014) utilized expert panel perspectives to understand better how collaboration impacts IS development. Ramim and Lichvar (2014) reported that the Delphi methodology allows consensus over the responses and informed judgment of the participants. Such, Gouglidis, Knowles, Misra, and Rashid (2016) leveraged SMEs to identify characteristics of information assurance (IA) techniques. Findings from Such et al. (2016) suggested that many IA techniques require senior consultants who are highly skilled in their subject areas (p. 125). Webler, Levine, Rakel, and Renn (1991) used groups of SMEs to evaluate risk management regulations, which helped to define dominant presumptions toward reducing risk.

For the development of an SRC survey, Trevelyan and Robinson (2015) actively encouraged the use of well-focused questions. Having well-focused initial statements reduces the burden on SMEs and the overall length of Delphi round(s) (Trevelyan & Robinson, 2015). During the Phase 1 Delphi round, structured survey questions were ranked on a 7-point Likert scale. The optimal number of scale categories for survey questions is between four to seven, with participants favoring seven (Trevelyan & Robinson, 2015). As a result, this research study used subject matter experts (SMEs) and a single iteration of the Delphi expert methodology to refine and clarify survey questions for the pilot study in Phase 2.

Phase 2

A research approach of this nature has many stages. Moreover, complex research projects such as those involving regulatory compliance often necessitate pilot studies to test how well-designed a survey instrument is (Avella, 2016). Phase 2 started with SMEs helping refine the SRC survey instrument from Phase 1 and then involved pilot testing of the SRC survey instrument. Tasks in Phase 2 included (a) conducting pilot study, (b) participant sample size and, (c) pilot study data analysis to test the reliability and validity of the initial SRC survey instrument.

Pilot study. Figure 4 illustrates the main focus of Phase 2, the pilot study. A pilot study, or pilot testing of a survey instrument, is considered a rigorous method of pretesting. Pilot studies can help identify where there are administrative issues, problematic questions, or unclear instructions within a survey instrument (S. Robinson, 2019; Ruel, 2018). According to Ruel (2018), pilot testing serves to improve a survey instrument’s face and content validity. Pilot testing is critical for online surveys, as it evaluates the flow and clarity of the survey instrument instructions as well as questions (Nardi, 2018b). The pilot study used Survey Monkey, an online survey-based platform.

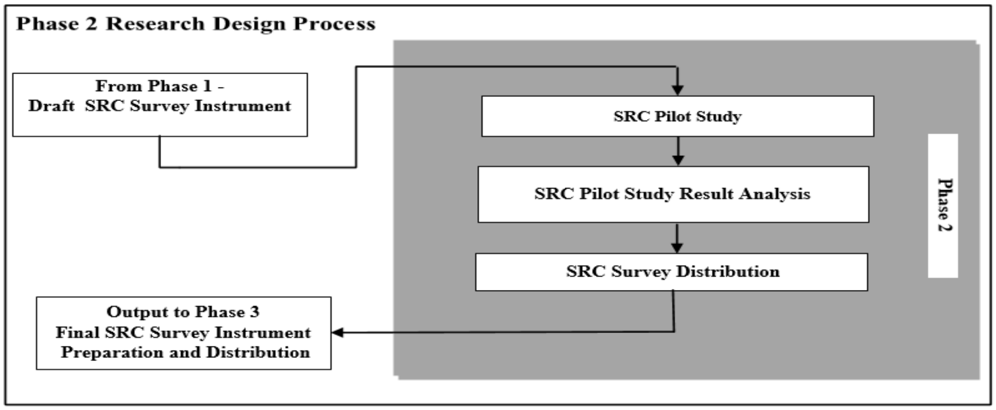

Phase 2 Research Design Process
From Phase 1 -
Draft SRC Survey Instrument
SRC Pilot Study
SRC Pilot Study Result Analysis
SRC Survey Distribution
Phase 2
Output to Phase 3
Final SRC Survey Instrument
Preparation and Distribution

Figure 4. Phase 2 Research Design and Process

Pilot sample size. There were several considerations and variables involved in the selection of the pilot study's participants and sample size (S. Robinson, 2019). Considerable debate exists as to what constitutes a proper sample size for pilot testing. S. Robinson (2019) suggested that a small and strategic sample of participants should be selected for the pilot study to pretest the survey instrument effectively. Kieser and Wassmer (1996) stated that 10-20 participants are sufficient to identify meaningful differences in groups. Additionally, cost and time considerations play a factor in pilot sample size selection (Fowler, 2014).

This research study utilized a single iteration pilot test based on a convenience sample of 15 CEs & BAs (Kieser & Wassmer, 1996). This convenience sample was selected based on known healthcare entities (CEs & BAs) and the project champions recommendation(s) (Ruel, Wagner, & Gillespie, 2016). A convenience sample selection of this nature afforded the ability to identify a cross-section of industry types, as well as various organizational sizes. After the pilot's sample population was selected, participants were contacted by the project champion's company and received the SRC pilot survey to complete. The pilot SRC survey instrument included comment areas, where pilot participants were encouraged to provide feedback. Empirical data and feedback from the SRC pilot-test were analyzed, with question modifications and adjustments to the survey instructions, completed were identified (See Appendix K).

Pilot data analysis. All statistical analyses were performed using SPSS v.24 for Windows. All of the analyses were two-tailed with a 5% alpha level. The 5% alpha is a common threshold for confidence levels in scientific research (Field, 2017). Demographic characteristics of the pilot study participants, the IVs, DV, as well as all survey questions were summarized using the mean, standard deviation, and range for continuous scaled variables, and frequency and percent for categorical scaled variables (Tabachnick & Fidell, 2019). One of the goals of the pilot study was to establish instrument internal consistency reliability using Cronbach's alpha statistical analysis (Tabachnick & Fidell, 2019). Cronbach’s alpha was used to measure the internal consistency reliability of the IV scale scores of motive (MT), characteristics and capacity (CC), regulator respect (RR), as well as deterrence factors(DT) (Tabachnick & Fidell, 2019). The Cronbach's alpha statistic is used to evaluate internal consistency reliability, with the common rule-of-thumb being, a Cronbach's alpha of 0.70 or higher indicates acceptable reliability (Tabachnick & Fidell, 2019). Once the data were analyzed, the SRC survey instrument question(s) and other modifications were instituted.

Instrument Development and Validation

Phase 2, illustrated in Figure 4, showed that the focus was on refining the SRC survey instrument via pilot study and, distributing the final SRC survey to participants. As previously mentioned, Appendix F, Tables F1 -F5 provided the constructs, descriptions, and supporting references adopted and developed for the SRC survey instrument. The development of constructs for this research study was firmly built on existing constructs within the literature, utilizing existing survey questions where possible, or developing questions with support from existing studies. Construct and survey questions sought to emphasize possible associations and interactions between factors enforcing or encouraging the perceived likelihood of SR compliance in CEs & BAs (Parker & Nielsen, 2017). The next step in Phase 2 distributed a final version of the SRC survey instrument to the population of interest.

Independent Variable Measures

Motives (MT): This score will be measured on a continuous scale with a range of 1-7. The score will be computed as the average of questions MT1-MT8 from the revised Parker and Nielsen (2017) questionnaire (Appendix C, Figure C1). Responses to the 8 survey questions were measured on a 7-point Likert-type scale ranging from 1 = Strongly Disagree to 7 = Strongly Agree. Thus, smaller scores indicate a perception among CEs & BAs that motives are less important with respect to the perceived likelihood of compliance with the HIPAA SR, while larger scores indicate a perception among CEs & BAs that motives are more important with respect to compliance with the HIPAA SR.

Characteristics and Capacities (CC): This score will be measured on a continuous scale with a range of 1-7. The score will be computed as the average of questions CC1-CC8 from the revised Parker and Nielsen (2017) questionnaire (Appendix C, Figure C1). Responses to the 8 survey questions were measured on a 7-point Likert-type scale ranging from 1 = Strongly Disagree to 7 = Strongly Agree. Thus, smaller scores indicate a perception among CEs & BAs CCs are less important with respect to the perceived likelihood of compliance with the HIPAA SR, while larger scores indicate a perception among CEs & BAs that CCs are more important with respect to compliance with the HIPAA SR.

Regulator Respect (RR): This score will be measured on a continuous scale with a range of 1-7. The score will be computed as the average of questions RR1-RR3 from the revised Parker and Nielsen (2017) questionnaire (Appendix C, Figure C1). Responses to the 3 survey questions were measured on a 7-point Likert-type scale ranging from 1 = Strongly Disagree to 7 = Strongly Agree. Thus, smaller scores indicate a perception among CEs & BAs that RR is less important with respect to the perceived likelihood of compliance with the HIPAA SR, while larger scores indicate a perception among CEs & BAs that RR is more important with respect to compliance with the HIPAA SR.

Deterrence Factors (DF): This score will be measured on a continuous scale with a range of 1-7. The score was computed as the average of questions DT1-DT15 from the revised Parker and Nielsen (2017) questionnaire (Appendix C, Figure C1). Responses to the 15 survey questions were measured on a 7-point Likert-type scale ranging from 1 = Strongly Disagree to 7 = Strongly Agree. Thus, smaller scores indicate a perception among CEs & BAs that deterrence factors (DF) are less important with respect to the perceived likelihood of compliance with the HIPAA SR while larger scores indicate a perception among CEs & BAs that DFs are more important with respect to compliance with the HIPAA SR.

Dependent Variable Measures

Perceived likelihood of complying with the HIPAA SR (PCH): This score was measured on a continuous scale with a range of 0 - 100. The score was obtained from question PC16 on the questionnaire. Question PC16 asks: “On a scale of 0 to 100, what is the perceived likelihood your organization is fully compliant to the SR regulatory standards, safeguards, and all implementation specifications?

Power calculations were performed using the G*Power v. 3.1.9.2 software. Power analysis "represents the probability that effects that actually exist have a chance of producing statistical significance" (Tabachnick & Fidell, 2019, p. 10). As discussed in the data analysis section, the RQ was tested using standard multiple linear regression analysis (MLR). However, it appears that there is no official consensus on the sample size formula used in logistic regression studies (Demidenko, 2007). Power analysis can be used to assess the population sample size needed for a statistically significant study (Tabachnick & Fidell, 2019).

Power analysis for MLR is based on the amount of change in R-squared attributed to the variables of interest (Tabachnick & Fidell, 2019). The variables of interest were the IVs of motives, characteristics and capacities, regulator respect, and deterrence factors. According to J. Cohen (2013), small, medium, and large effect sizes for hypothesis tests about R-squared are: f^2 = 0.02, 0.15, and 0.35, respectively. A sample size of n = 400 with a 0.05 alpha level produces 80% power to detect a small effect size of f^2 = 0.03. Appendix G, Figure G1 shows the results of the G*Power settings used for this analysis. The G*Power analyses result demonstrated that a sample size of approximately 400 is adequate to detect small effect sizes for H1 – H4, making this a statistically significant and robust study.

Phase 3

Figure 5 illustrates three critical activities for Phase 3 of this research study that of (a) prescreening and pre-analysis, (b) empirical assessment and analysis, and (c) results in the write-up, including a discussion regarding the findings and data. Multiple Linear Regression (MLR) data analysis was used to empirically assess the RQ and relationships in the conceptual model illustrated in Figure 1.

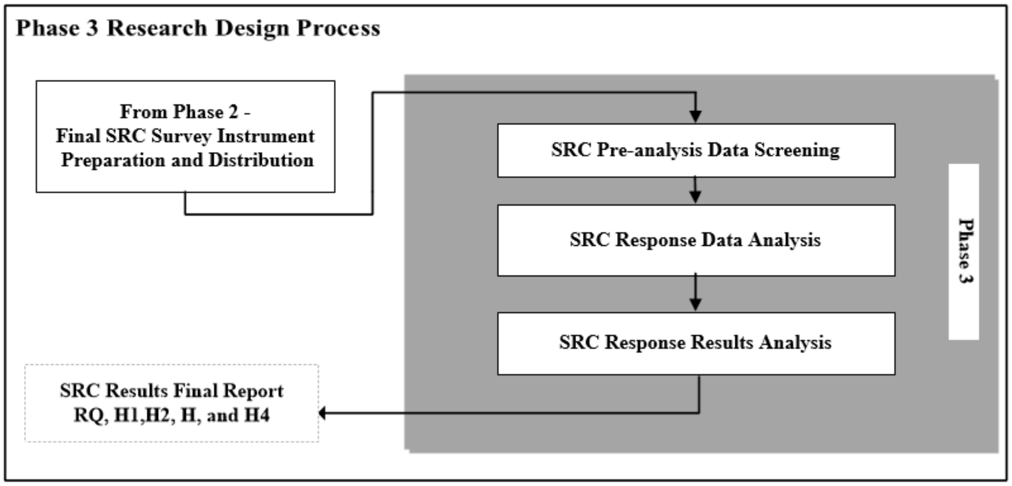

Phase 3 Research Design Process
From Phase 2 -
Final SRC Survey Instrument
Preparation and Distribution
SRC Pre-analysis Data Screening
SRC Response Data Analysis
SRC Response Results Analysis
SRC Results Final Report
RQ, H1,H2, H, and H4
Phase 3

Figure 5. Phase 3 Research Design and Process

Pre-analysis Data Screening. Pre-analysis, data accuracy, and other pre-screening activities were performed in Phase 3. Pre-analysis data screening activities were required to ensure that conclusions were based on valid data (Mertler & Reinhart, 2016). The pre-analysis data screening activities were (a) verifying the overall accuracy, (b) checking for missing data, (c) screening and correcting for outliers and, (d) full data analysis (Mertler & Reinhart, 2016).

Verify the accuracy of data. The start of the pre-analysis data screening process began with verifying the accuracy of the data (Mertler & Reinhart, 2016). Directly importing respondent data from Survey Monkey data extracts into International Business Machines (IBM) Statistical Package for Social Sciences (SPSS) statistical software, removing any chance for data entry errors or omissions. Furthermore, SPSS statistical frequencies options provided descriptive statistics of Means, Standard Deviations, as well as Minimum and Maximum values, which were utilized for reasonable accuracy checks of data (Tabachnick & Fidell, 2019). Moreover, it was helpful to use SPSS's graphing abilities to review the data visually. Histograms, box plots, and scatter plots aided in identifying gaps as well as helping spot errors in the frequency, distribution, and sufficiency of the data points (Mertler & Reinhart, 2016).

Checks for missing data. A total of 172 (5.7%) responded to the invitation and provided informed consent. Among the 172 respondents, 114 (66.3%) completed the entire survey. The final sample response size for this study was n = 114. When dealing with missing data, the critical thing was to figure out if the data is randomly missing or if there is some underlying pattern or reason for its absence (Tabachnick & Fidell, 2019). Visual inspection of all the sampled population responses revealed no missing data points. If inspection of the data provides no discernible pattern, manual verification and testing may be required (Tabachnick & Fidell, 2019). Manual inspection of sample population responses also revealed that there were no data points missing.

Tabachnick and Fidell (2019) stated that another procedure for handling missing data is to "simply to drop any cases with them" (p. 57). The sampled population responses (n=114) revealed that no cases needed to be dropped. Furthermore, Tabachnick and Fidell (2019) stated that it is possible, should a value be missing, that its predictive ability lies in its absence. Moreover, Tabachnick and Fidell (2019) stated that "deletion is a reasonable choice if the pattern appears random" (p. 62) and, to avoid substitution of data. Additionally, performing the analysis with and without the missing data is also highly recommended (Tabachnick & Fidell, 2019).

Screening for outliers. Tabachnick and Fidell (2019) have defined an outlier as a "…case with such an extreme value on one variable (a univariate outlier) or such a strange combination of scores on two or more variables (multivariate outlier) that it distorts statistics" (p. 62). The pre-analysis statistical assumptive tests leveraged in this study and detailed in Chapter 4 revealed no outliers or extreme leverage values that needed to be addressed in the sample population participating in this research study.

Data Analysis Strategy

All statistical analyses were performed using SPSS v.24 for Windows. All of the analyses were two-tailed with a 5% alpha level. The 5% alpha is a standard threshold for confidence levels in scientific research (Field, 2017). Demographic characteristics of the SRC survey instrument sample, along with the descriptive statistical tests (outlined in the Instrument Development and Validation section), were conducted for the IVs, DV, as well as all survey questions. Demographic and descriptive SRC survey instrument results were summarized using the mean, standard deviation, and range for continuous scaled variables and frequency and percent for categorical scaled variables (Tabachnick & Fidell, 2019). In addition, Cronbach's alpha was used to measure the internal consistency reliability of the IV scale scores (Tabachnick & Fidell, 2019).

The research study's RQ was tested using multiple linear regression (MLR) as a result of the assumptions being satisfied. MLR is useful for testing and estimating the strength of relationships between measured variables and unobserved constructs (Creswell & Creswell, 2018b; Tabachnick & Fidell, 2019). Individually, six assumptions were evaluated prior to conducting an MLR analysis.

The first assumption was that the independent variables collectively have a linear relationship with the dependent variable (Osborne & Waters, 2002). This assumption was evaluated by inspecting a scatterplot of the studentized residuals versus the unstandardized predicted values (Tabachnick & Fidell, 2019). The second assumption was that each independent variable was individually linearly related to the dependent variable (Osborne & Waters, 2002). This assumption was evaluated by the inspection of partial regression plots of each independent variable individually versus the dependent variable (Tabachnick & Fidell, 2019). The third assumption was that there is homogeneity of variance (Homoscedasticity)(Osborne & Waters, 2002). This means the variance in the dependent variable was approximately the same for all values of the independent variable. This assumption was evaluated by inspection of the same scatterplot used to evaluate the first assumption, the studentized residuals versus the unstandardized predicted values (Tabachnick & Fidell, 2019). The fourth assumption was there is no multicollinearity (Osborne & Waters, 2002). This assumption was evaluated by inspecting the variance inflation factors (VIF) (Tabachnick & Fidell, 2019). Multicollinearity can occur when the variables in the study are very highly correlated. When variables are highly correlated, they essentially are two measures of the same thing, thus redundant measures (Tabachnick & Fidell, 2019). The fifth assumption was that there are no unusual data points, meaning, no significant outliers, high leverage points, or influential data points (Osborne & Waters, 2002). Evaluation of potential outliers was conducted by inspection of casewise diagnostics and studentized deleted residuals (Tabachnick & Fidell, 2019). Evaluation of potential leverage points was be conducted by inspection of leverage values. Evaluation of potential influential values was done by inspection of Cook’s distance values (Tabachnick & Fidell, 2019). The sixth assumption was that the error terms have a roughly normal distribution. This assumption was evaluated by inspection of two different graphs: 1) a histogram of the Regression Standardized Residuals, and; 2) A normal P-P plot of the Expected Cumulative Probability values versus the Observed Cumulative Probability values (Osborne & Waters, 2002; Tabachnick & Fidell, 2019).

If any of the assumptions were severely violated, then transformations of the independent and dependent variables were to be tried in attempt to remedy the problems. If transformations were ineffective, the standard multiple linear regression would be performed without transformations, and any violations of assumptions would be reported as potential limitations of the study (Tabachnick & Fidell, 2019).

If the assumptions for MLR were satisfied and two or more of the independent variables were statistically significant, it would be concluded that two or more independent variables collectively better predict the perceived likelihood of meeting compliance, then any single independent variable alone. The equation of the model was reported, and statistically, significant regression coefficients were interpreted. The R-square and effect size (f^2) for the final model was presented and interpreted. Those IVs whose results were statistically significant were deemed to be a significant predictor of the DV.

Hypothesis 1-4 was initially tested using Pearson’s correlation coefficient. However, all the necessary assumptions for Pearson’s correlation statistic were not satisfied. The first assumption for Pearson’s correlation statistic was that there is a linear relationship between the independent (e.g., motive) and the dependent variable (e.g., perceived likelihood of complying with HIPAA SR). This assumption was evaluated by inspection of a scatter plot between the independent and dependent variables. If the scatter plot shows strong evidence that the linearity assumption is violated, then the non-parametric correlation statistic, Spearman's rho, will be used instead of Pearson's correlation statistic since the Spearman's rho statistic is more robust against violations of the linearity assumption.

The second assumption for Pearson's correlation statistic to be valid is that there are no significant outliers. The same scatter plot was used to evaluate this assumption, as mentioned above. If no data points fall far outside the general pattern of the data points, the assumption of no outliers was considered satisfied. If there are extreme outliers, those data points were removed from the analysis.

The third assumption is that both the independent and dependent variables had a roughly normal distribution. This assumption was evaluated by the inspection of histograms of the independent and dependent variables. If the normality assumption was violated, Spearman's rho would be used instead of Pearson's correlation statistic since the Spearman's rho statistic is more robust against violations of the normality assumption.

If the Pearson correlation coefficient was statistically significantly different than zero, it would be concluded there is a correlation between perceptions and behaviors toward achieving compliance (e.g., motive) and the perceived likelihood of meeting SR compliance among CEs & BAs. The strength and direction of the correlation will be reported and interpreted, as well. However, the assumptions necessary to utilize the Pearson correlation coefficient statistical analysis were violated. As a result, Spearman's

Rank Correlation was used instead to assess and test H1-H4 empirically. To further complement and augment the Spearman's Rank Correlation analysis of the predictive power of the IVs, multiple linear regression (MLR) was also used. MLR is useful for testing and estimating the strength of relationships between measured variables and unobserved constructs

Ethical Considerations

The Institutional Review Board (IRB) at Nova Southeastern University (NSU) approved this research study. The voluntary nature of participation was made clear to all participants via informed consent. Additionally, participant information was not stored or tracked due to Survey Monkey's anonymous response survey features (SurveyMonkey, 2019). Typically, Survey Monkey's email invitations track the participant's email address and Internet Protocol (IP) address. However, Survey Monkey's anonymous response survey feature turns off this tracking, thus reinforcing the participant's anonymity.

Formats for Presenting Results

Tables 3, 4, and Figure 6 are formatting examples of how empirical data is presented in this research study. Formatted figures and charts, similar to Tables 3, 4, and Figure 6, presents results from this research study's statistical analysis. This research study's actual results are offered in chapters 4 and 5, as well as the appendices.

Table 3.

Example Presentation of Descriptive Statistics for the IVs and DV.

	N			Std.	Minimu	Maximu
	Valid	Missing	Mean	Deviation	m	m
IV1 [a]	41	0	3.0061	0.98661	0.00	4.00
IV2 [a]	41	0	3.1037	0.82154	0.50	4.00
IV3 [a]	41	0	3.4146	0.86170	0.25	4.00
DV [b]	41	0	2.8720	1.04302	1.42	5.58

[a] Independent variables:

[b] Dependent variable:

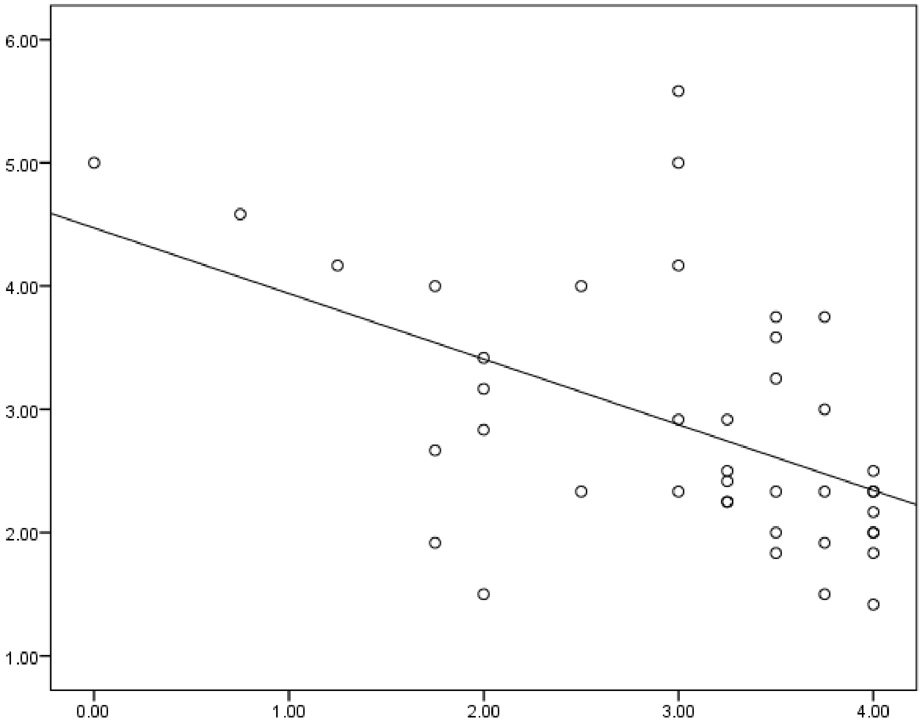


Figure 6. Example Scatterplot for Presenting Results.

Table 4

Example Multiple Linear Regression for Presenting Results

	Unstandardized Coefficients		Standardized Coefficients		
Model [a, b]	B	Std. Error	Beta	t	*p*-value.
(Constant)	4.768	0.477		9.991	<0.0005
IV1 [a]	-0.040	0.022	-0.246	-1.831	0.075
IV2 [b]	-0.546	0.142	-0.517	-3.839	<0.0005

a. Independent Variable:

b. $F(2, 38) = 8.69$; $p = 0.001$.

Resource Requirements

Ancillary resources required for this research study included: computer, Internet access, Microsoft Word, and Microsoft Excel, IBM SPSS statistical software, and a Survey Monkey account. This research leveraged human subjects, which required advance approval from the Institutional Review Board (IRB) at Nova Southeastern University (NSU).

Summary

This section detailed the research methodology, design, and approach toward investigating compliance perceptions in CEs & BAs operating in the U.S., and why they remain challenged to comply with the HIPAA SR regulatory strategy. According to Fowler (2014), the two main goals of a robust methodology are to minimize errors and address how well the research study's design addresses the research questions and goals. Figure 2 illustrates the overall three-phase design of this research study. The main objective of Phase 1 was to develop an SRC survey-based data collection instrument.

This instrument was clarified and refined via the use of the Delphi expert methodology via SME's responses. Phase 2’s primary objectives were to pilot test the SRC survey instrument, refine, and then distribute a final version to the sampling population of interest. Phase 3’s objectives were to perform an empirical assessment of the participant responses to answer this research study’s RQ, along with addressing its hypotheses(H1-H4). After statistical analysis of the dataset, the RQ and hypotheses were discussed and addressed in the final report write-up.

Chapter 4

Results

Overview

This chapter presents statistical and empirical analyses of results obtained for the perceived likelihood of compliance (PC1) as affected by motives (MT), characteristics and capacities (CC), regulator respect (RR), and deterrence factors (DT). A visualization of the three-phased approach applied in this survey-based research study is located in the methodology section of Chapter 3. For greater clarity, the following sections mirror the structure of Chapter 3.

In Phase 1, after a literature review, a Security Rule Compliance (SRC) survey instrument was developed, with the help of subject matter experts (SMEs). Phase 2 involved a pilot study of the SRC survey instrument to test and refine survey questions, as well as to determine the validity and reliability of the survey instrument. The SRC survey instrument was further refined in Phase 2 (via a pilot study) for distribution in Phase 3. In Phase 3, the SRC survey instrument was administered to the sample population. Appendix H provides the final SRC instrument. Results were then analyzed and interpreted to address the research question (RQ) and the individual hypotheses (H1-H4). Phase 3 concluded with results write-up and final reporting.

Phase 1 – SMEs Feedback and Findings

Figure 3, Chapter 3, illustrated the tasks involved in Phase 1. The objectives of Phase 1 were: (a) exploration of literature, (b) identification of a research problem, and (c) development of a research question. The research question led to the creation of an SRC survey-based instrument, pulling from available literature and previous research. Constructs (Appendix F, Tables F1 - F5) were identified and developed to assess RQ and H1-H4. Next, subject matter experts (SMEs) helped validate and refine the SRC survey instrument (Appendix H). After receiving approval from the Nova Southeastern Institutional (NSU) Review Board (NSU-IRB) (Appendix I), Phase 1 involved: (a) identification and solicitation of 15-18 SMEs; (b) initial survey solicitations, and (c) analysis of SME responses. Using Delphi expert methodology, the SRC instrument was further refined. Invitations or requests for SME participation were sent to 34 healthcare, cybersecurity, and compliance professionals working in CEs & BAs across the United States. Invitations were also sent to previous Office for Civil Rights (OCR) directors. Of the 34 invitations sent, 18 SMEs (53%) agreed to be part of the research study and offered professional feedback and input.

SME participation was anonymous; however, various healthcare executives, a compliance attorney, along with a previous Office for Civil Rights director, self-identified their participation by providing additional feedback via email. Feedback from 18 SMEs resulted in minor question changes, verbiage clarifications, and ethical recommendations.

Table 5 highlights SME feedback and recommendations. SMEs strongly recommended that the following (Table 5) SRC survey instrument questions be removed or altered due to potential legal/ethical implications and redundancy of construct question measures. All SME feedback can be seen in Appendix J. As a result, the SRC survey instrument was re-ordered for distribution as a pilot study. Appendix K illustrates the survey question numbering changes from the pilot to the final SRC.

Table 5

SMEs - SRC Survey Instrument Recommendations

Security Rule Compliance - Motive		**Comments**
MT2. Superficial adoption of the SR provides substantial advantages.	MT2. Superficial adoption of the SR provides substantial advantages.	Removed due to ethical considerations - based on attorney advice.
MT4. Our organization agrees with the SR regulatory strategy, its policy objectives, and the principles that underpin it.	MT4. My organization agrees with the SR regulatory strategy and its underlying principles of: -- Comprehensiveness. (addresses all aspects of security) -- Scalability- (so it can be effectively implemented by CEs & BAs of all types and sizes), -- Technologically Generic. (not linked to specific technologies).	Altered to clarify SR principles better.
Page 6: Security Rule Compliance - Deterrence Factors		
DT7. The risk of an SR violation being detected is low in our organization).	DT7. The risk of an SR violation being detected is low in our organization.	Removed redundant with DT5.
DT9. Our organization falls outside of the priority targets for SR compliance enforcement).	DT9. Our organization falls outside of the priority targets for SR compliance enforcement.	Removed redundant with DT5-8.
DT14. Sanctions for violations of SR compliance will be imposed quickly by OCR).	DT14. Sanctions for violations of SR compliance will be imposed quickly by OCR.	Removed timeliness is too subjective.

Phase 2 – Pilot Study Feedback and Findings

A convenience sample of 26 participants were invited to participate in the pilot study. Participants included professionals working in healthcare, cybersecurity, legal, and risk and compliance across the U.S. The primary purpose of the pilot study was to evaluate the internal consistency reliability of the independent variables (IVs): (a) motive (MT), (b) characteristics and capacities (CC), (c) regulator respect (RR) and, (d) deterrence factors (DT). In order to identify meaningful differences between groups, 10 - 20 participants are ideal for a pilot sample size (Kieser & Wassmer, 1996). Cost and time considerations also play a factor in the pilot sample size (Fowler, 2014). Fifteen professional CEs & BAs completed the pilot study (58%), which helped establish the internal consistency reliability of the SRC survey instrument.

Pre -Analysis – Reverse Coding and Computing Scale Scores

Before computing IV scale scores, each survey question (e.g., MT1 - MT3) needed to be reviewed for reverse coding and coded in such a way that a response of Strongly Agree means more motivation to comply with the SR and a response of Strongly Disagree means less motivation to comply with the SR (Creswell, 2019). Reverse coding means to change a response of Strongly Disagree (with a value of 1) to Strongly Disagree (to a value of 7) (Cenfetelli, Bassellier, Cenfetelli, & Bassellier, 2009). For example, reverse coding was necessary for CC4. CC4 was worded as "*The SR is too complex to comply with or to implement fully,"* due to the verbiage and its original intent, CC4 required reverse coding so that the value of 7 = Strongly *Disagree*. In doing so, a larger score (response to the survey item) remains consistent with more motivation toward compliance with the SR. Table 6 illustrates the survey questions that required reverse coding.

Table 6

IVs that required Reverse Coding

IV#	SRC Survey Question
CC4	The SR is too complex to comply with or to implement fully.
DT2	My organization is at a lower risk of being investigated by the Office for Civil Rights (OCR) for SR violations than other organizations.
DT3	The likelihood that my organization will be subjected to HIPAA inspection due to an SR breach or violation is low.
DT4	A routine OCR investigation would not reveal any SR violations at my organization.
DT5	My organization has sufficient documentation of SR compliance for OCR investigations.
DT8	For SR compliance investigations, OCR has a track record of providing technical assistance and requiring corrective action plans instead of settlements and civil money penalties.
DT9	The risk of settlements or civil money penalties is low, even if being caught in a breach can be validated.

The internal consistency reliability of the survey instrument was measured using Cronbach’s alpha (Tabachnick & Fidell, 2019). Cronbach’s alpha was computed based on average inter-item survey question responses and the number of items used (Tabachnick & Fidell, 2019). A Cronbach's alpha of 0.70 or higher indicates acceptable reliability (Tabachnick & Fidell, 2019). Table 7 shows the results of Cronbach’s alpha analysis of the pilot study’s independent variables.

Table 7

Pilot Study Findings - Cronbach's Alpha for Independent Variables

HIPAA Entity	Cronbach's alpha (n = 15)	Number of items
Motive (MT)	.90	3
Characteristics and Capacities (CC)	.77	8
Regulator Respect (RR)	.73	3
Deterrence Factors (DT)	.72	10

Motive (MT). A Cronbach's alpha of .90 is considered an excellent indicator of internal consistency reliability in the measurement of the independent variable (Tabachnick & Fidell, 2019). Statistical analysis determined that in order to achieve this level of reliability, it was necessary to evaluate the MT construct based on survey questions MT2, MT3, and MT4. In addition to achieving a reliability score of excellent, computing the MT score based on these constructs helped reduce the overall time required to complete the SRC survey. Several SMEs indicated that the survey was too long. One SME stated, "about halfway through, I glazed over." As a result of the SME's feedback, and pilot study analyses, the MT variable was pared down to a more robust and reliable measure.

Characteristics and Capacities (CC). A Cronbach's alpha of .77 is considered an indicator of good internal consistency reliability of an independent variable

(Tabachnick & Fidell, 2019). Statistical analysis determined that changes to the survey, for the CC construct, were not necessary.

Regulator Respect (RR). A Cronbach's alpha of .73 is considered an acceptable indicator of internal consistency reliability in an independent variable (Tabachnick & Fidell, 2019). In order to achieve this alpha, survey questions RR2, RR3, and RR4 were included.

Deterrence Factors (DT). A Cronbach's alpha of .72 is considered an acceptable indicator of internal consistency reliability in an independent variable (Tabachnick & Fidell, 2019). The DT construct was analyzed using survey questions DT1, DT3-6, and DT8-12. The final version of the SRC survey and amendments to the initial version can be found in the appendices (Appendix H and Appendix K, respectively).

Phase 3 – SRC Distribution and Data Analysis

An online survey instrument titled: Security Rule Compliance (SRC) was designed, piloted, tested, and delivered via SurveyMonkey, an online web-based format. As a result, no manual input of participant data was conducted, eliminating response data input errors. The population of interest was healthcare covered entities and business associated (CEs & BAs) operating in the U.S. After consulting with the project champion, it was estimated that the project champion's company had 400 clients and access to 2100 individuals working in various healthcare areas, executive working groups, and healthcare compliance arenas. On September 30, 2019, the organizations below were given (with advanced approval) the SRC survey instrument. Two thousand five hundred clients and association members were invited to participate in the SRC survey research study. Healthcare and information security professional associations included:

- AEHIS - Association for Executives in Healthcare Information Security
- CHIME - College of Healthcare Information Management Executives
- HCCA - Health Care Compliance Association
- SIRA - Society of Information Risk Analysts.

A variety of factors can influence research participant survey response rates (Fan & Yan, 2009). Industry reports have provided a wide variety of data concerning typical (expected) survey response rates. For example, Fryrear (2015), from SurveyGizmo, reported that an average survey response rate for an external survey is between 10-15%, while others, like Baruch & Holtom (2008), claimed rates as high as 35.7%. At the onset of this study, a survey response rate of approximately 16% (400 responses) was expected.

The SRC survey instrument (See Appendix H) was sent to CEs & BAs, as noted above, between 09/30/2019 and 10/30/2019. However, around the midpoint of the collection dates (10/18/2019), it became apparent that the SRC survey instrument was experiencing low participant response rates. Although numerous factors could contribute to low response rates, it was determined that the specialized focus on the SR, and the fact that almost all research about regulatory compliance is highly sensitive, made participants apprehensive about completing the survey (Losoncz, 2017). As a result, the pool of participating organizations was widened. The following organizations were approached, and permission was granted to distribute the SRC survey:

- CHWG - Cyber Healthcare Working Group
- HIoT - HIoT Security Executive Summit

- IAPP - International Association of Privacy Professionals
- MIC3 - Michigan Cyber Civilians Corp

The new participating organizations, and their respective approvals, were submitted to NSU-IRB over various dates in October 2019 as, “Additional Participating Organizations.” With the added organizations, the SRC survey was distributed to approximately 3000 potential participants**.**

Data Analysis Strategy

All statistical analyses were performed using SPSS v.24 for Windows. All of the analyses were two-tailed with a 5% alpha level. The 5% alpha is a standard threshold for confidence levels in scientific research (Field, 2017). Multiple linear regression (MLR) was utilized to answer the RQ effectively, and all required assumptions were met. Individually, six assumptions were evaluated prior to conducting the MLR analysis. Demographic characteristics of the SRC survey instrument sampling population, along with descriptive statistical tests (outlined in the Instrument Development and Validation section), were conducted for the IVs, DV, and all survey questions. Demographic and descriptive results were summarized using the mean, standard deviation, and range, for continuous scaled variables and frequency and percent for categorical scaled variables (Tabachnick & Fidell, 2019). In addition, Cronbach’s alpha was used to measure the internal consistency reliability of the IV scale scores (Tabachnick & Fidell, 2019). Originally, Pearson’s correlation was planned to answer H1-H4 effectively; however, various assumption tests, to validate the use of Pearson’s correlation were violated. As a result, Spearman’s rho correlation coefficient was validated and used to assess the associative relationships between the IVs (MT, CC, RR, and DT) and DV (PC1).

Data Analysis - Descriptive Statistics for Demographic Variables

A total of approximately 3,000 CEs & BAs were invited to participate in the SRC research study. A total of 172 (5.7%) responded to the invitation and provided informed consent. Among the 172 respondents, 114 (66.3%) completed the entire survey. The final sample response size for this study was n = 114. Among the 114 study participants, 75 (65.8%) reported their organization's primary HIPAA classification as a covered entity (CE), while 39 (34.2%) reported their organization as a business associate (BA). Appendices L through Q, provide the SRC instrument's response findings, including descriptive and frequency statistics. Due to the large volume of descriptive statistics and frequency results, only a select few statistical findings that are worthy of mentioning have been included within the body of this paper.

The sample population represented participation from a total of 29 different U.S. states, as indicated by the location of their organization's headquarters (Appendix L). The sample population's participation revealed the most frequent U.S. states were Michigan, (n=35; 30.7%) and Texas (n=11; 9.6%). The remaining 27 states had between one and seven study participants. The Michigan-centric sample participation of the study was not surprising, as this was a convenience sample of known contacts in healthcare and cybersecurity areas.

A total of 57 participants (50%) reported that their organization's business model was Non-Profit (Appendix L). The business model reporting was an even split between non-profit and for-profit organizations. This result was not surprising, given the complexities of healthcare financial structures, along with the constant pressure of value-based versus volume-based business models (Angst et al., 2017; Vogenberg, 2019).

Additional pressures on healthcare systems have led to consolidation, which routinely changes financial structures and organizational shapes of CEs & BAs (Vogenberg, 2019).

A total of 74 participants (64.9%) reported their gender as male, 30 (26.3%) reported their gender as female, and 10 (8.8%) preferred not to report their gender. The age distribution (reported in age ranges) was: 4 participants (3.5%) [20 to 29 years]; 9 participants (7.9%) [30 to 39 years]; 30 participants s (26.3%) [40 to 49 years]; 43 participants (37.7%) [50 to 59 years]; and 18 participants (15.8%) [60 years or older]. Ten participants (8.8%) declined to report their age. Furthermore, 88% of respondents (n = 101) had at least a 4-year college degree, while 46.5% (n = 53) had a graduate or doctoral degree. The convenience sample population had multiple years of high-level industry experience, as 82% (n = 94) reported having six or more years of experience in healthcare cybersecurity, compliance/risk, finance, or legal areas. An additional 41.2% (n = 47) reported having 16 or more years of experience in healthcare. See Appendices L – Q for detailed demographic statistics and frequency tables for all SRC survey items.

Data Analysis - Descriptive Statistics for the IVs (MT, CC, RR, DT) and DV (PC1)

Table 8 shows descriptive statistics of valid sample responses (n=114) for MT, CC, RR, and DT, along with PC1. There were no sample participants missing data; as a result, all responses (n=114) were leveraged. All IVs were scored on a range from 1 to 7, and all four IVs had an average between 4.46 (DT) and 5.944 (MT). All four IVs had an average above the midpoint (4.0), indicating that study participants placed a relatively high level of importance on MT, CC, RR, and DT factors, as they may relate to HIPAA SR compliance regulatory strategy and regulations. Similarly, the DV (PC1), had a potential range of 0 to 100. The average PC1 score was 72.9, indicating those study participants on average perceived their organization as having a relatively high probability of meeting HIPAA SR regulations.

Table 8

Descriptive Statistics for the IVs and DV.

	N	Missing	Mean	Median	Std. Deviation	Min	Max
Motives [a]	114	0	5.94	6	0.7756	3.3	7
Characteristics and Capacities [a]	114	0	5.04	5.125	0.978	2.3	7
Regulator Respect [a]	114	0	4.88	4.667	0.9431	3	7
Deterrence Factors [a]	114	0	4.46	4.5	0.6499	3.1	6
Probability of Organization’s Compliance [b]	114	0	72.9	80	22.544	0	100

[a] Independent Variables

[b] Dependent Variable

Data Analysis – Internal Consistency Cronbach’s Alpha for the IVs

After reverse coding, the constructs (Table 6), Cronbach’s alpha was used to empirically assess the internal consistency reliability of the items included in the SRC survey. Table 9 details the results of a second Cronbach’s alpha internal consistency reliability analysis. The results showed that MT, CC, and RR had satisfactory internal consistency reliability, alpha = 0.70 or above (Cohen, 1988). However, the DT’s internal consistency reliability coefficient was reduced to .57, versus its initial calculation of 0.72 in the pilot study.

Table 9

Initial Cronbach's Alpha of the Four Independent Variables.

Variable	Cronbach's alpha (n = 114)	Number of items
Motives	0.70	3
Characteristics and Capacities	0.87	9
Regulator Respect	0.69	3
Deterrence Factors	0.57	10

The DT6 construct was omitted from the final statistical analysis; by doing so, the number of DT survey items decreased to 9 items. As Table 10 illustrates, this omission generated a Cronbach's alpha internal consistency reliability score for the overall DT constructs of 0.71, indicating acceptable internal consistency reliability (Cohen, 1988).

Table 10 details the adjusted Cronbach's alpha statistical analysis with internal consistency reliability coefficients for all IVs measured by the SRC survey instrument. Table 10 shows that except for RR's Cronbach's alpha score, the MT, CC, and DT variables achieved a Cronbach's alpha of 0.70 or higher. This level of Cronbach's alpha score typically indicates acceptable internal consistency reliability (Cohen, 1988). Because the Cronbach's alpha score for RR (0.69) was only slightly below 0.70, it was not considered a major threat to the internal consistency reliability of the SRC instrument, and it was used in preliminary study findings (Plummer & Tanis Ozcelik, 2015; van Griethuijsen et al., 2015)

Lower values for Cronbach’s alpha internal consistency reliability do not always imply that an instrument is unsatisfactory, as Plummer and Ozcelik, 2015 and Van Griethuijsen (2015) research have previously reported. Van Griethuijsen et al. (2015) performed a cross-national student study and justified the use of several Cronbach alpha values below the commonly accepted level of 0.70 (p. 588). With 114 respondents, the revised Cronbach’s alpha statistic demonstrated that the SRC survey instrument was reliable and fit for its intended purpose (Taber, 2018). After validating the SRC survey instrument, RQ and H1-H4 were addressed.

Table 10

Adjusted Cronbach’s Alpha for the Four IVs (DT6 removed).

Variable	Cronbach's alpha (n = 114)	Number of items
Motives	0.70	3
Characteristics and Capacities	0.87	9
Regulator Respect	0.69	3
Deterrence Factors	0.71	9

This study’s unique theoretical model allowed for the examination of factors that exist in complex regulatory compliance research (Losoncz, 2017; Parker & Nielsen, 2011, 2017). Ultimately, this research study provided statistical analyses and addressed the relationship between MT, CC, RR, and DT and the perceived likelihood of compliance with HIPAA SR (PC1), among healthcare CEs & BAs operating in the U.S. The following RQ and H1-H4 were analyzed and addressed:

RQ: Do the factors of (a) motives; (b) characteristics and capacities; (c); regulator respect and (d) deterrence predict the perceived likelihood of compliance with the HIPAA SR among healthcare CEs & BAs operating in the U.S?

H1: Motive is a significant predictor toward the perceived likelihood of complying with HIPAA SR in CEs & BAs.

H2: Characteristics and capacities are a significant predictor toward the perceived likelihood of complying with HIPAA SR in CEs & BAs.

H3: Regulator respect is a significant predictor toward the perceived likelihood of complying with HIPAA SR in CEs & BAs.

H4: Deterrence is a significant predictor toward the perceived likelihood of complying with HIPAA SR in CEs & BAs.

To address and investigate the relationship between the IVs and the DV, and to ultimately answer this study's RQ, multiple linear regression (MLR) was conducted. MLR can help researchers better understand the functional and collective relationships between the IVs and DV. MLR was used to find an equation and statistical model that could best predict the DV as a function of the IVs. MLR was used to create a regression line for the DV with given values for the IVs (Tabachnick & Fidell, 2019). Furthermore, MLR was utilized to empirically investigate whether or not any single IV, or combinations of IVs, could explain variations in the DV (Osborne & Waters, 2002).

RQ – MLR Pre-analysis and Findings

In order to effectively answer the RQ, pre-analysis of the data was performed to ensure that all MLR assumptions were met. Specifically, six assumptions were evaluated prior to conducting the MLR analysis. The first assumption was that the independent variables had a linear relationship with the dependent variable (Osborne & Waters, 2002). This assumption was evaluated by inspecting a scatterplot of the studentized residuals versus the unstandardized predicted values (Tabachnick & Fidell, 2019). The studentized residuals formed a roughly horizontal band, satisfying this assumption (Appendix R, Figure R1).

The second assumption was that each independent variable was individually and linearly related to the dependent variable (Osborne & Waters, 2002). This assumption was evaluated by visual inspection of partial regression plots for each independent variable, versus the dependent variable (Tabachnick & Fidell, 2019). All four partial regression plots showed a roughly linear relationship, so this assumption was considered satisfied (Appendix R, Figures R2-R5).

The third assumption was that there was homogeneity of variance (homoscedasticity) (Osborne & Waters, 2002). This means that variance in the DV was approximately the same for all IV values. This assumption was evaluated by inspection of the same scatterplot used to evaluate the first assumption: studentized residuals versus unstandardized predicted values (Tabachnick & Fidell, 2019) (Appendix R, Figure R1). With the exception of several outliers for the studentized residuals (low end of the vertical axis), the data points indicated a roughly horizontal pattern, indicating that variation in the residuals was constant over different values of the predicted values. Therefore, this assumption was considered satisfied (Appendix S, Figure S1).

The fourth assumption was that there was no multicollinearity (Osborne & Waters, 2002). As O'Brien (2007) purported, Variance Inflation Factor (VIF) values are widely used as measures to understand the degree of multi-collinearity an IV has with another IV in a regression model. Multicollinearity can occur when the variables in the study are highly correlated with each other. When variables are highly correlated, they essentially measure the same thing, making them redundant measures (Tabachnick & Fidell, 2019). Generally, any VIF greater than 2.0 is indicative of multicollinearity. Previous authors have used a cut-off of 10.0 (O'Brien, 2007). Table 11 presents the testing of this assumption by inspecting the VIF values for all IVs (Tabachnick & Fidell, 2019). The VIF values for all IVs were all below 2.0, which satisfied the fourth assumption.

Table 11

MLR - Variance Inflation Factors (VIF) to evaluate Multicollinearity.

DV MLR Model	Collinearity Statistics
	VIF
Importance of Motives with respect to (HIPAA) Security Rule (SR)	1.489
Importance of Characteristics and Capacities with respect to (HIPAA) Security Rule (SR)	1.520
Importance of Regulator Respect with respect to (HIPAA) Security Rule (SR)	1.118
Importance of Deterrence Factors with respect to (HIPAA) Security Rule (SR)	1.133

The fifth assumption was that there were no unusual data points, significant outliers, high leverage points, or other influential data points contained within the data set. Any of these data points could alter the correct interpretation of the results (Osborne & Waters, 2002). An outlier is an observation with a large residual (Liu, Milton, & McIntosh, 2016). A leverage point is an observation that has a value that is far from the mean (Liu et al., 2016).

Evaluation of potential leverage points was conducted by inspection of leverage values (Appendix T). Evaluation of potential outliers was conducted by inspection of casewise diagnostics, and assessing studentized deleted residuals, as shown in Appendix T (Tabachnick & Fidell, 2019). Casewise diagnostics only identified one outlier; it was just barely an outlier (Appendix T). The studentized deleted residuals identified only three outliers, and they were not very extreme outliers in the sense they were just slightly below -3.0 (Appendix T). Appendix T displays evaluations for the top three studentized deleted residuals, leverage values, and Cook's values. Potential leverage points were conducted by inspection of leverage values. Influential values were analyzed by inspection of Cook's distance values. Influential values of potential leverage points were evaluated by inspection of leverage values. Leverage is based on how much the observation's value differs from the mean value of that observation (Lane, n.d.).

Appendix T shows the three largest leverage values that may adversely affect the MLR model. The top three leverage values in the observations (n = 114) were less than 0.13. Leverage values less than 0.20 are not concerning (Tabachnick & Fidell, 2019). Evaluation of potential influential values was done by inspection of Cook's distance values as determined from SPSS Casewise Diagnostic statistical routine. (Tabachnick & Fidell, 2019). Cook's distance statistic identifies observations that may have had undue influence on the overall MLR model (Tabachnick & Fidell, 2019).

Table 12 shows that one study participant (Case 77) had a casewise diagnostic of -3.064, just below the cut-off of +/- 3.00. The cut off of +/- 3.00 is known as the Empirical Rule (Tabachnick & Fidell, 2019). The Empirical Rule states that for a normal distribution, nearly all the observations will fall within three standard deviations of the mean (Tabachnick & Fidell, 2019). Case 77 had a standardized residual value of -3.064; however, it was not considered large enough to have a significant influence on the results. Case 77 was included in all the analyses. All three leverage values had studentized deleted residuals slightly less than -3.0, which was not considered significant enough to warrant the deletion of their responses (Creswell, 2019).

Table 12

Casewise Diagnostics[a]

Case Number	Std. Residual		Predicted Value	Residual
77	-3.064	0	59.54	-59.536

Cook's distance is used in regression analysis to find influential outliers in a set of independent (predictor) variables (Cook, 1977). Cook's distance values were all below 0.16. A value greater than 1.0 is cause for concern (Cook, 1977). Thus, none of the observations were considered influential. Taken together, the three diagnostics, outliers, leverage, and influential values did not support the removal of any study participants. The fifth assumption was considered satisfied (Appendix T).

The sixth assumption was that the error terms have a roughly normal distribution. This assumption was evaluated by inspection of two different graphs: Figure 7, a histogram of the Regression Standardized Residuals, and Figure 8, a normal P-P plot of the Expected Cumulative Probability values versus the Observed Cumulative Probability values (Osborne & Waters, 2002; Tabachnick & Fidell, 2019).

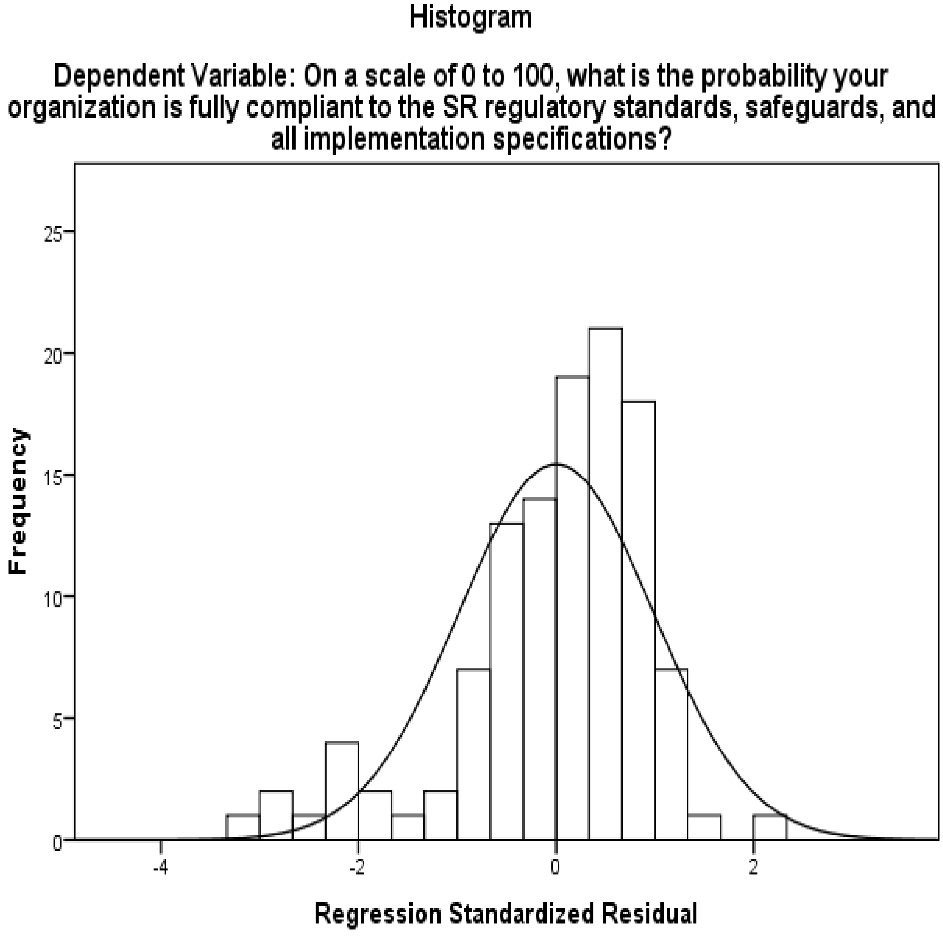


Figure 7. Histogram of Regression Standardized Residuals to evaluate the Normality Assumption.

The histogram in Figure 7 closely resembles a normal distribution, providing support to the normality assumption. Figure 8 Normal P-P plot showed that the data points fell near a diagonal line, further supporting an assumption of normality. Taken together, Figure 7’s histogram and Figure 8’s Normal P-P plots showed the sixth assumption to be satisfied. Since all of the MLR pre-analysis assumptions were satisfied, standard (forced) MLR analysis was performed as outlined initially in Chapter 3.

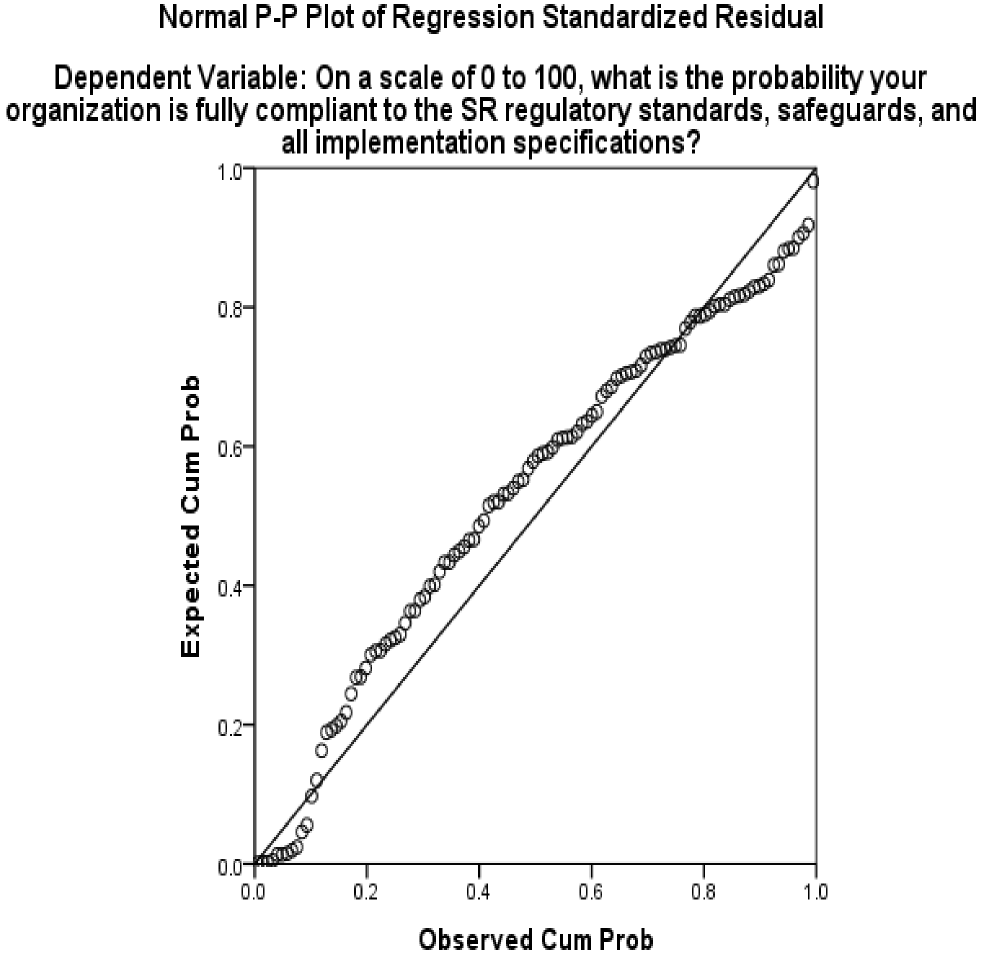


Figure 8. Normal P-P plot of the Expected Cumulative Probability values versus the Observed Cumulative Probability values to further evaluate the normality assumption.

MLR can help determine which, if any, combination of IVs best predicts the DV (Creech, 2016). Standard or forced MLR analysis (SPSS default), includes all IVs into the MLR regression model, without any decision as to the order of importance to the DV (Field, 2017). Field (2017) noted that hierarchal and stepwise MLR operations might be prejudiced by random variations in data, making reproducible results difficult. Furthermore, Studenmund (2017) stated that the most appropriate MLR method for theory testing is standard (forced) MLR. Table 13 shows the output from SPSS, a standard MLR model summary table. The MLR summary table reports on the strength of the relationships between the IVs the DV. Table 13 also provides essential summary information about the statistical model's fit to the data: the values of *R*, $R^{2,}$ and the adjusted (adj) R^2. These values helped determine how well the regression model fits the data (Dhakal, 2018).

Table 13

Percentage of the total variance in PC1 explained by the full model (R^2)

Model [a]	R	R Square	Adjusted R Square	Std. Error of the Estimate
	0.532[a]	0.283	0.257	19.433

a. Predictors: (Constant), Importance of Deterrence Factors with respect to (HIPAA) Security Rule (SR), Importance of Motives with respect to (HIPAA) Security Rule (SR), Importance of Regulator Respect with respect to (HIPAA) Security Rule (SR), Importance of Characteristics and Capacities with respect to (HIPAA) Security Rule (SR).

The column labeled R, contains the multiple correlation coefficient, a measure of the quality of the prediction of the DV (PC1) (Creswell, 2019). R is always positive and takes on a value between zero and one (Field, 2017). The interpretation of R is similar to the interpretation of the correlation coefficient; it measures the strength of the linear association (Laerd Statistics LLC., 2019). The closer the value of R to one, the stronger the relationship between the IVs and DV (Tabachnick & Fidell, 2019). The R-value of 0.532 indicated an above-average level of prediction in the model. However, the next value R^2 (R Squared) is a more popular method of assessing model fit (Laerd Statistics LLC., 2019)

R^2 represents how close the observed data points were to the predicted (fitted) regression line's data points, often called the coefficient of determination (Aron, Coups, & Aron, 2017). The four IVs, in this model, explained 28% of the total variance in PC1 ($R^2 = 0.28$). In general, the higher the R^2 value, the better the data fits the model, however as Frost (2017) noted, studies attempting to understand human behavior often have R^2 values less than 50% because a person's perceptions and behaviors are harder to predict than physical methods. Moreover, Furthermore, Field (2017) noted, a low R^2 value does not indicate whether a regression model is adequate or not, as a low R^2 can still be a good fitting model. Research conducted by Miaou, S. P., Lu, A., & Lum, H. S. (1996) on traffic accidents posited the variably and pitfalls of using R^2 values as a goodness of fit measurement. Subsequently, with R^2 values lower than 50%; the adjusted R^2 value should be reviewed as another assessment for model fitting analysis (Dhakal, 2018)

The adjusted R^2 (Adj R^2) indicates the amount of variance in the dependent variable that can be explained by the independent variables, after taking into consideration the number of independent variables. It provides an idea of how generalizable a model is to the population being studied. Table 16 shows $R^{2 =}$ 0.283 and Adj R^2 = 0.257. The adjusted R^2 is less than R^2, as expected. In other words, with the addition of the four IVs, into the model, Adj R^2 = 0.257, explained 25.7% of the total variance in PC1 as compared to the mean of the DV model without IVs included.

R^2 provides input into a model's effect size (f^2). R^2 is a quantitative result used to calculate effect size ($f^2 = R^2/(1- R^2$)(Cohen, 1988). Effect size (f^2) measures the size (magnitude) of relationships; the larger the effect size (f^2), the more associative the relationship. According to Cohen (1988), small, medium, and large effect sizes for hypothesis tests are: f^2 = 0.02, 0.15, and 0.35, respectively. The effect size for this model was f^2 = 0.39, a large effect size, which provided further evidence that the model was a good predictor of the DV (PC1).

Table 14 provides the statistical significance of the overall MLR model. According to Tabachnick and Fidell (2019), a model's total variance is the sum of the Regression and Residual variances. Regression variances can be explained by IVs, and variance not explained by the IVs is called Residual, or Error. Overall, the model was statistically significant based on the result of PC1 = $F(4, 109) = 10.77$; $p < 0.001$. The model was statistically significant at predicting PC1.

Table 14

Statistical Significance for the full model.

Full MLR Model	Sum of Squares	df	Mean Square	F	*p*-value.
Regression [a]	16267.065	4	4066.766	10.77	<0.001[b]
Residual	41161.505	109	377.628		
Total	57428.570	113			

a. Dependent Variable: On a scale of 0 to 100, what is the probability your organization is fully compliant to the SR regulatory standards, safeguards, and all implementation specifications?
b. Predictors: (Constant), Importance of Deterrence Factors with respect to (HIPAA) Security Rule (SR), Importance of Motives with respect to (HIPAA) Security Rule (SR), Importance of Regulator Respect with respect to (HIPAA) Security Rule (SR), Importance of Characteristics and Capacities with respect to (HIPAA) Security Rule (SR).

Based on Table 14, at least one of the independent variables (MT, CC, RR, or DT) was significantly related to PC1: $F(4, 109) = 10.77$; $p < 0.001$. The F statistic is an intermediate calculation, along with degrees of freedom (df), used to compute a p-value for the predictive ability of the overall model (Creech, 2016). If $p < 0.05$, then the model is statistically significant, which indicates that at least one of the independent variables was statistically significant (Creech, 2016; Creswell, 2019). With MLR, the p-value of the F-test indicates whether the model is statistically significant (Tabachnick & Fidell, 2019). The model for this study was statistically significant; $p < 0.001$, indicating that it was a good fit for the (Cohen, 1988).

Table 15 shows the statistical significance of the individual IVs, as well as the standardized and unstandardized Beta coefficients. Although some debate exists as to which regression coefficients (unstandardized, standardized, or both) should be presented, this research study presents both (Aron et al., 2017). The first row in Table 15 gives the regression constant (48.256) and other statistics related to the constant. In addition, there are rows of unstandardized (B), and standardized (Beta) regression coefficients for each of the IV have been included.

Unstandardized coefficients (Colum B, Table 15) indicate how much the DV varies with a specific IV when controlling for all other IVs. Standardized coefficients (beta weights) are shown in the Beta column. Beta coefficients measure how much the DV increases (in standard deviations) when an IV increases by one standard deviation (holding the other variables in the model constant) (Dhakal, 2018). These measures helped to rank the IVs based on their contribution to the model (Dhakal, 2018). The predicted value for PC1 was 48.256, when all the IVs were held at zero. Based on this, calculation, the perceived likelihood of compliance with the HIPAA SR among healthcare CEs & BAs operating in the U.S, averaged, 48.3%.

Table 15

Statistically Significant IVs and beta coefficients

Model [a]	Unstandardized Coefficients		Standardized Coefficients	t	*p*-value
	B	Std. Error	Beta		
(Constant)	48.256	22.786		2.118	0.036
Importance of Motives with respect to (HIPAA) Security Rule (SR)	-3.403	2.876	-0.117	-1.183	0.239
Importance of Characteristics and Capacities with respect to (HIPAA) Security Rule (SR)	13.037	2.305	0.566	5.656	<0.001
Importance of Regulator Respect with respect to (HIPAA) Security Rule (SR)	-2.051	2.050	-0.086	-1.001	0.319
Importance of Deterrence Factors with respect to (HIPAA) Security Rule (SR)	-2.428	2.995	-0.070	-0.811	0.419

a. Dependent Variable: On a scale of 0 to 100, what is the probability your organization is fully compliant to the SR regulatory standards, safeguards, and all implementation specifications?

Table 15 shows the model's estimate of regression coefficients and the associated t-statistic and p-values. The t-statistic, and its associated p-value, measure the extent to which a coefficient is statistically significant (Creswell, 2019). P-values were calculated using the t statistic and degrees of freedom to examine which IVs were statistically significant. These calculations indicated whether or not a significant association existed between the IV and the DV. Beta coefficient were also used to indicate whether an IV was an important indicator of the DV (Tabachnick & Fidell, 2019).

To address the RQ, and whether or not MT, CC, RR, and DT were related to the perceived likelihood of compliance, standardized (Beta) regression coefficients values were further analyzed and interpreted. For a given IV, the coefficient (Beta) can be interpreted as the average effect on the DV (outcome) of a one-unit increase in IV, while keeping all other factors fixed. Of the four IVs, only CC was statistically significant, indicating that it had the most substantial relationship with the DV.

The MLR model equation was: PC1 = 48.26 – 3.40*MT + 13.04*CC + 2.05*RR - 2.43*DT. Where PC1 indicated the probability that an organization was, or would be, fully compliant to SR regulatory standards, safeguards, and implementation specifications. When controlling for MT, RR, and DT, PC1 is expected to increase by 13.04 points for every 1-point increase in CC. The CC value (13.04) explained much of the variation in PC1, as compared to the other 3 IVs (MT, RR, and DT), which together were not enough to explain a significant amount of variation in PC1.

RQ Results Summary

Multiple regression was run to predict PC1 from MT, CC, RR, and DT. The model significantly predicted PC1, $F(4, 109) = 10.77$; $p < 0.001$, $R^2 = 0.283$. MLR assessment determined whether or not combinations of the IVs better predicted the DV, as compared to a single IV. Only CC was a statistically significant predictor of PC1. These results suggest that MT, RR, and DT's do not have a statistically significant relationship with PC1.

Furthermore, MLR statistical analysis beta coefficients showed that MT, CC, and RR were not statistically significant (confirmed by beta coefficients that could not be distinguished from zero). CC was the only and strongest predictor of the DV. Further analyses were performed to discover any nuanced associations between the IVs and DV (H1-H4).

Correlation analysis and MLR analysis complement each other (Creech, 2016). Performing a standalone MLR can give the impression that only one IV is predictive of the DV, whereas all four IVs may have statistically significant correlations with the DV. Additional analyses were needed to discover any associations between the IVs and DV. For this purpose, correlation analysis was performed to address H1-H4 and help further explain each IV's associative strength and relationships with the DV.

H1-H4 – Pre-analysis and Findings

To address H1- H4 hypotheses, Pearson's correlation was planned. The Pearson correlation coefficient ranges between -1 and 1 (Creswell, 2019). The further away the calculated value is from zero, the stronger the linear relationship between the two variables in question. Furthermore, a scatterplots' line of direction, as noted by the positive or negative integer's sign (- or +), denotes linear direction. A positive linear-direction indicates that as one variable's value increases, the other variables tend to increase as well (Creswell & Guetterman, 2019). A negative linear value (-) indicates that as one variable increases, the other variable tends to decrease (Creswell & Guetterman, 2019). A perfect linear value (1 in absolute value) indicates that each one of the variables can be entirely explained by the linear function of the other (Creswell, 2019). Visual inspection of Appendices U-X showed that the linear assumption was satisfied. However, in order to use Pearson’s statistical analysis, there were several pre-analysis data screening and statistical assumption checks that had to be validated or met (Creswell, 2019). These assumptions included: (a) a linear relationship, (b) no significant outliers, and (c) that the data set had a roughly normal distribution. All of these assumptions were evaluated in order to correctly conduct, apply, and interpret Pearson’s correlation (Creswell, 2019). Table 16 shows the results of the Pearson correlation coefficient assumption tests for H1-H4.

Table 16

Pearson's Correlation Assumption Checks of H1-H4

Hypothesis	IVs and DV	Linear Relationship	Outliers	Normal Distribution
H1	MT and PC1	Y	V	V
H2	CC and PC1	Y	V	V
H3	RR and PC1	Y	V	V
H4	DT and PC1	Y	V	V

Note; Y = Yes, the check passed, V= Violates, the check failed.

In all cases, the first assumption, a linear relationship exists between the individual IVs and DV passed. This assumption was evaluated by visually inspecting the scatter plots between the IVs and DV (See Appendices U - X). The second assumption for Pearson’s correlation is that there are no wayward or extreme outliers between the IVs, as outliers can have a substantial effect on the Pearson correlation coefficient and may ultimately lead to incorrect or different conclusions (Field, 2017) (See Appendices U - X). The second assumption between the IVs and DV that no significant outliers existed was evaluated in Appendices U through X. As Table 16 illustrates, this assumption was violated on account of several values of PC1 being less than 20, whereas most of the data points were well above 20 (See Appendices U - X).

The third assumption for Pearson’s correlation is that both the IVs & DV have a roughly normal distribution (Creswell & Guetterman, 2019). Typically, a visual check or inspection of a histogram can identify skewness or asymmetry (Tabachnick & Fidell, 2019). The assumption of normality was violated, as illustrated in Table 16. Based on the evaluations described above, the assumptions for Pearson’s correlation were not satisfied. As a result, Pearson’s correlation was inappropriate to use for statistical analysis of H1-H4. Instead, Spearman’s Rank (rho) Correlation Coefficient was used.

Spearman’s rho does not require normal distributions, and it is impervious to outliers (Mukaka, 2012). According to Weir (2018), Spearman’s rho is a statistical measure of the monotonic strength of a relationship between paired data, with its interpretation similar to that of Pearson (the closer Spearman’s rs is to the absolute values of +/- 1, the stronger the monotonic association). Spearman’s rs is calculated by converting observations to ranks, rank-ordering variables, and then performing Pearson’s correlation statistic on the ranks. For example, data points like 1, 2, 3, 4, 500, when ranked as 1, 2, 3, 4, 5, eliminating outliers.

The only requirement for Spearman’s rho is that the relationship between the two variables is monotonic (Creswell, 2019). To be visually monotonic data need to display either an increasing or a decreasing trend, but not a bell curve relationship (Tabachnick & Fidell, 2019). The monotonic relationship assumption was visually evaluated for H1-H4 by inspection of the same scatterplots used to test for Pearson’s linearity and outliers. See scatterplots and histograms (a) H1 - Appendix U, Figures U1 - U3, (b) H2 - Appendix V, Figures V1 – V3, (c) H3 - Appendix W, Figures W1-W3, (d) H4 - Appendix X, Figures X1 – X3 for reference.

Spearman's rho was used to assess H1-H4 empirically. Although no guidelines exist as to what constitutes a small, medium, or large effect size or Spearman's rho, it is a commonly accepted practice to use Pearson's correlation values to interpret Spearman's rho (Creswell & Guetterman, 2019). The closer the value is to 0, the weaker the relationship. The closer the value is to 1 in absolute value, the stronger the relationship (Ramsey, 1989). A Spearman's rho correlation greater than 0 indicates a positive relationship (as one variable increases the other tends to increase also) while a Spearman's rho correlation less than 0 indicates a negative relationship (as one variable increases, the other variable tends to decrease)(Gideon & Hollister, 1987). As Xiao, Ye, Esteves, and Rong (2016) purported, Spearman's correlation can describe the strength of the association using the common Pearson's correlation guide for the absolute values of $r_{s;}$ that is ."0.1 - 0.3 weak, 0.3 - .05 moderate, 0.5 -1.0 strong" (pg.3868).

Spearman's rho correlation coefficient was used to assess the IVs (MT, CC, RR, and DT) associative relationship to the DV (PC1). Each hypothesis was individually analyzed and addressed:

H1: Motive is a significant predictor toward the perceived likelihood of complying with HIPAA SR in CEs & BAs.

H2: Characteristics and capacities are a significant predictor toward the perceived likelihood of complying with HIPAA SR in CEs & BAs.

H3: Regulator respect is a significant predictor toward the perceived likelihood of complying with HIPAA SR in CEs & BAs.

H4: Deterrence is a significant predictor toward the perceived likelihood of complying with HIPAA SR in CEs & BAs.

H1 - Findings

Figure 9 is a scatter plot of the relationship between PC1 and MT and illustrates the result of Spearman's correlation analysis. A statistically significant, positive association between PC1 and MT, r_s (112) = 0.25; p = 0.006 was observed. A positive association between PC1 and MT was observed, suggesting that as MT increases, the perceived likelihood of compliance with the HIPPA SR (PC1) also increases. Even though MT showed a statistically significant association, the observed correlation of r_s (112) = 0.25; p = 0.006 was considered a relatively weak correlation.

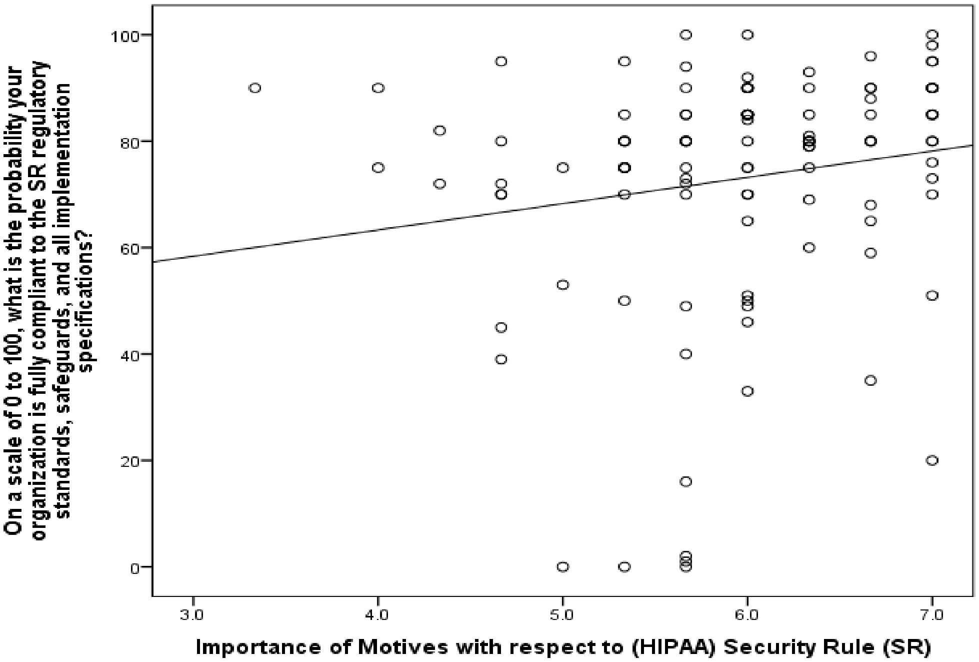


Figure 9. H1- Spearman's rho Scatter Plot of PC1 and Motive (MT) among healthcare CEs & BAs operating in the U.S. Spearman's rho: $r_s(112) = 0.25$; $p = 0.006$.

H2 - Findings

Figure 10 depicts a Spearman’s rho correlation scatter plot of the relationship between PC1 and CC. Figure 10 shows evidence of a strong association and correlation between the PC1 and CC variable. Spearman’s correlation analysis showed a statistically significant positive correlation between PC1 and CC, $r_s(112) = 0.51$; $p < 0.001$. These results suggested that as Characteristics and Capacities increase, the perceived likelihood of compliance with the HIPPA SR also increases. The observed correlation of $r_s(112) = 0.51$; $p < 0.001$ was considered a strong correlation and predictor of DV.

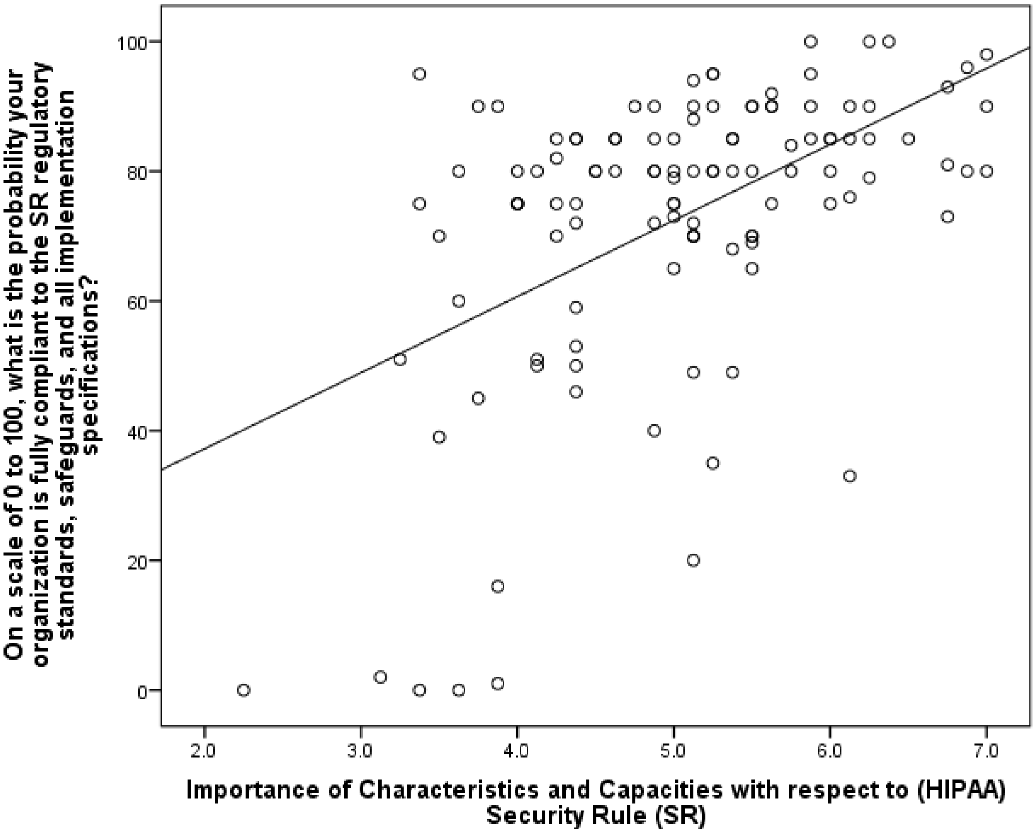


Figure 10. H2 - Spearman’s rho Scatter Plot of PC1 and CC among healthcare CEs & BAs operating in the U.S. Spearman’s rho: $r_s(112) = 0.51$; $p < 0.001$.

H3 - Findings

Figure 11 shows a scatter plot of the correlation between PC1 and RR. Little evidence of a correlation existed between these two variables. Spearman's correlation analysis showed a negligible to non-existent correlation between PC1 and RR, *rs*(112) = 0.09; p = 0.36.

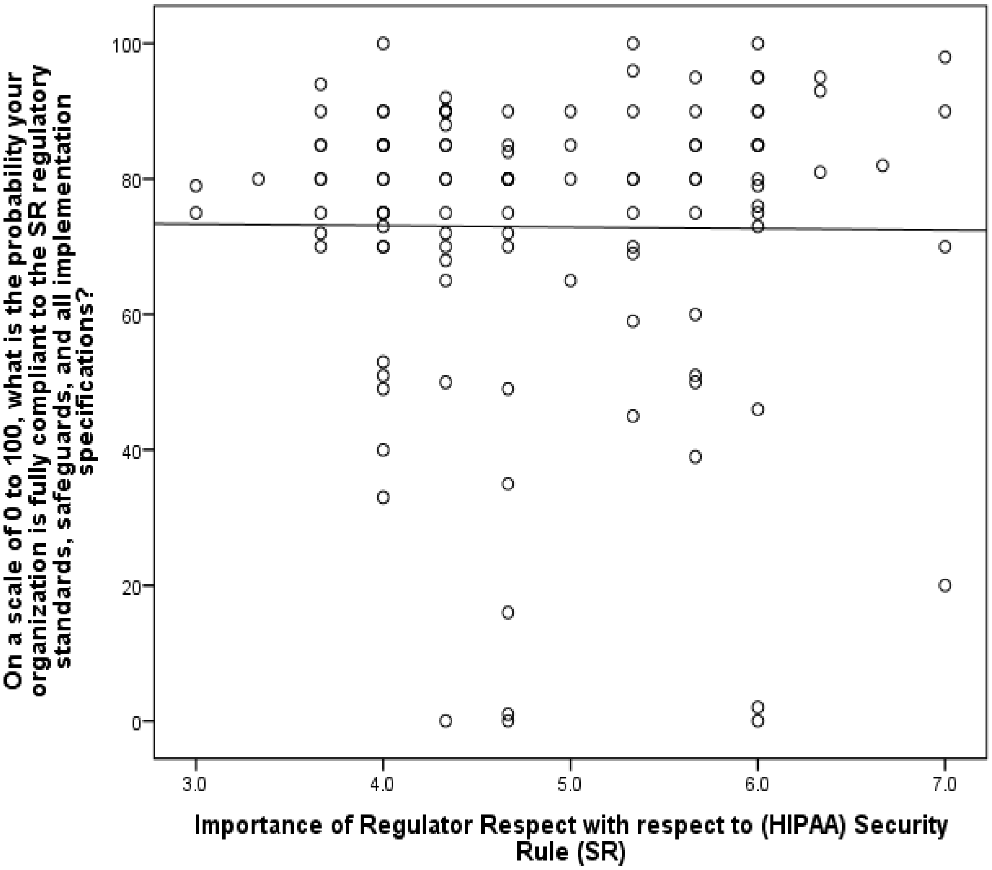


Figure 11. H3 - Spearman's rho Scatter Plot of PC1 and RR among healthcare CEs & BAs operating in the U.S. Spearman's rho: $r_s(112) = 0.09$; $p = 0.36$.

H4 - Findings

Figure 12 is a scatter plot of the relationship between PC1 and DT. This figure showed evidence of a negative correlation between the two variables. The results of Spearman's correlation analysis showed a statistically significant negative correlation between PC1 and DT, $r_s(112) = -0.21$; $p = 0.022$. The results suggest that as DT increases, PC1 decreases. Given that Spearman's rho correlation coefficient can range from -1 to +1, the observed correlation of $r_s(112) = -0.21$ was considered a weak correlation and was considered a weak predictor of DV.

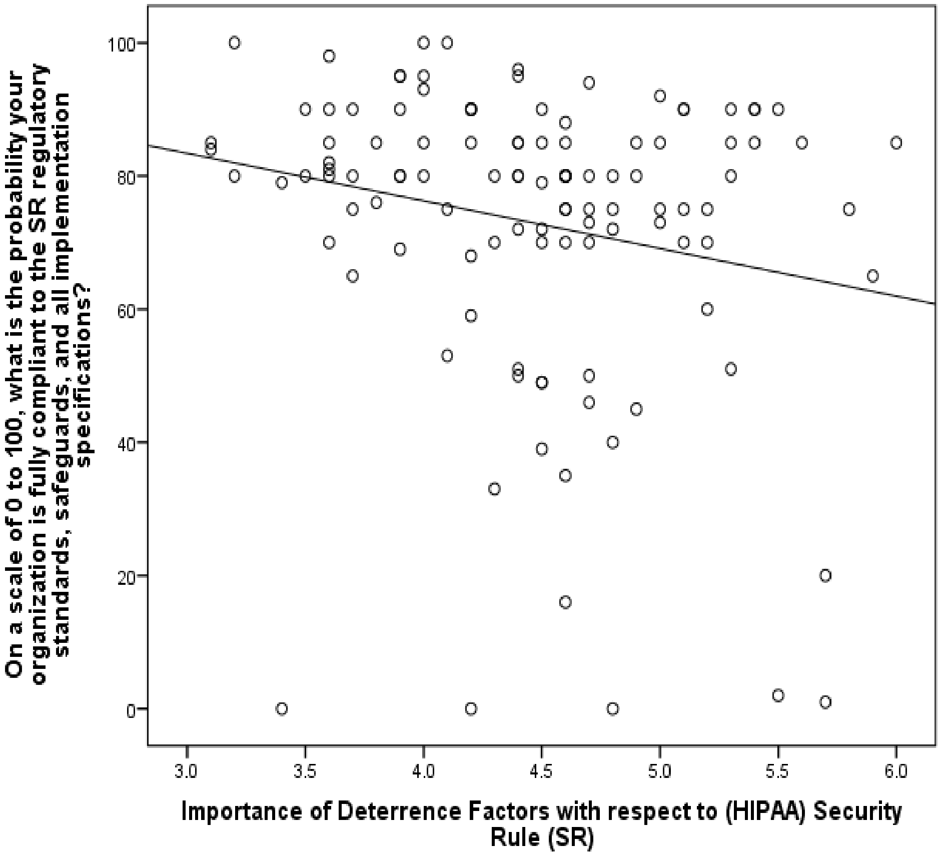


Figure 12. H4 - Spearman's rho Scatter Plot of PC1 and DT among healthcare CEs & BAs operating in the U.S. Spearman's rho: $r_s(112) = -0.21$; $p = 0.022$.

H1-H4 - Results Summary

Spearman’s rho correlation coefficients for H1-H4 are summarized in Table 17. Spearman’s (rs) correlation coefficient was performed to ascertain whether or not MT, CC, RR, or DT were statistically significant predictors of the perceived likelihood of compliance with the HIPPA SR in CEs & BAs.

Table 17

Results of Spearman’s ($r_{S)}$ Correlation of DV and IVs

Hypotheses	IV	df	r_s	*p*-value.
H1	MT	112	0.25	0.006
H2	CC	112	0.51	0.001
H3	RR	112	0.09	0.36
H4	DT	112	-0.21	0.022

Note: N=114, DV = PC1

Motive (MT), although statistically significant ($p > 0.05$), was weak to moderate ($r_s = 0.25$) in its associative or predictive strength. Regulator Respect (RR) was not statistically significant; there was almost no correlation ($r_s = 0.09$) between PC1 and RR. Characteristics & Capacities (CC), however, showed a strong statistical significance (r_s =0.51) and a positive correlation with the dependent variable (PC1). Finally, Deterrence Factors (DT) showed a statistically significant, negative correlation (r_s =-0.21). This negative correlation was expected, as DT efforts on behalf of government agencies increases, the perception of compliance to the SR would be expected to decrease.

Results - Summary

MLR was used to determine whether combinations of MT, CC, RR, and DT better predicted PC1 than any single IV alone. The statistical analysis demonstrated that only CC was a statistically significant predictor of PC1. The correlation between PC1 and CC ($r_s = 0.51$) was so much stronger than MT ($r_s = 0.25$); RR ($r_s = 0.09$), and DT ($r_s = -0.21$), that it explained a majority of the variation in PC1.

Spearman’s empirical analysis showed statistically significant positive correlations between PC1 and MT and PC1 and CC. A negative correlation existed between PC1 and DT. There was no correlation between PC1 and RR. MT, RR, and DT were all considered weak predictors of PC1, as CC had the strongest associative correlation.

Chapter 5

Conclusions, Implications, Recommendations, and Summary

Conclusions

Protecting the privacy and integrity of electronic protected health information (ePHI) is paramount in today's data-driven healthcare arena. Compliance with the HIPAA Security Rule (SR) regulatory strategy requires CEs & BAs to analyze their environment and take measures toward elevating and safeguarding ePHI. This research study provided a unique theoretical model that investigated the effects motives (MT), characteristics & capacities (CC), regulator respect (RR), and deterrence factors (DT), have on the perceived likelihood of SR compliance (PC1).

Frequency analysis on all four of the IVs showed that, on average, the 114 SRC study participants placed a relatively high level of importance on MT, CC, RR, and DT factors in regard to meeting HIPAA SR compliance regulations. Similarly, frequency analysis performed on the DV (PC1), indicated, on average, that 114 study participants perceived their organization to have a relatively high probability of meeting HIPAA SR regulations.

Multiple linear regression (MLR) analysis provided statistical insight, in that out of the four independent variables, only CC was statistically significant and had substantial explanatory value when predicting values for PC1. The interpretation of the

MLR model (when controlling for MT, RR, and DT), PC1 is expected to increase by 13.04 points for every one-point increase in CC. MT, CC, and DT were all correlated with PC1, with CC having the strongest correlation, but two or more of the independent variables did not add up to collectively predict (PC1) than CC alone. Moreover, Spearman's rho correlation assessment showed a statistically significant and robust positive correlation between PC1, and CC, providing further evidence that as Characteristics and Capacities increase the perceived likelihood of compliance to the HIPPA SR tends to increase as well. There was a statistically significant positive association, yet a weak explanatory association between PC1 and MT. This positive association suggests that as MT increases, the perceived likelihood of compliance with the HIPPA SR among healthcare CEs & BAs operating in the U.S may tend to increase as well.

Empirical analysis showed there was not a statistically significant correlation between PC1 and RR. The relationship between PC1 and RR was considered statistically weak or negligible. There was a negative correlation between PC1 and DT. As deterrence increases, the perceived likelihood of compliance with the HIPPA SR among healthcare CEs & BAs operating in the U.S tends to decrease. This inverse relationship between DT and PC1 makes sense, as an increase in governmental deterrence efforts and actions (i.e., audits, sanctions, and civil monetary penalties, etc.) may increase CEs & BAs concerns with SR compliance posture, especially if regulatory action were to take place.

To summarize, MLR analysis showed that out of the four independent variables, only characteristics and capacities was statistically significant. Correlation analysis showed a statistically significant, positive correlation between PC1 and MT, CC, and a negative correlation between PC1 and DT. There was a non-existent correlation between PC1 and RR. This research study offered unique insight toward understanding HIPAA SR compliance in CEs & BAs and evaluated the subtly nuanced or deeply intertwined factors that exist in regulatory compliance research (Losoncz, 2017; Parker & Nielsen, 2011 2017).

Implications & Recommendations

Table 18 outlines the CC construct, question emphasis, and participant responses. Review of the participant CC construct responses was imperative (considering the strength of the CC to PC1 relationship) to better understand the implications and possible recommendations resulting from this study.

Table 18

Characteristics & Capacities Response Emphasis

SRCSurvey Question#	Question Emphasis	Strongly Agree and Agree %	Strongly Agree and Agree Count	Strongly Agree and Agree Rank
CC1	Business Model	72.8%	83	7
CC2	SR Awareness	70.2%	80	6
CC3	Mgmt. Support	56.1%	64	5
CC4	SR Complexity	14%	16	8
CC5	SR Funding	31.6%	36	1
CC6	SR Tech Expertise	39.5%	45	4
CC7	Org Focus	32.5%	37	2
CC8	Hdw/Soft/Systems	34.2%	39	3

Note: N=114

CC1 and CC2 in Table 18 show that CEs & BAs understand that the SR is vital to their organization’s business model and that there appears to be an overall awareness of the SR regulatory strategy within an organization. Furthermore, CC4 demonstrated that only 14% of the respondents felt the SR was too complicated. This response indicated that a majority (86%) of respondents felt the complexity of SR regulatory mandates did not hinder compliance with the SR regulatory strategy. Collectively, CEs & BAs were aware of the SR and understood that the SR plays an essential part in their business model (CC1-CC3). Complexities of the SR regulatory strategy do not inhibit perceptions of compliance to the SR. However, when reviewing all of the past OCR settlements, resolution agreements and corrective action plans, human error is high on the root cause analysis list, as well as the lack of a comprehensive SR risk analysis for all ePHI that an entity accessed, creates, receives, stores, and transmits. Differences between OCR investigations and this research study findings bear further discussion.

The strength of the SR is that by design, it was built to be future proof. Future proof means that it was intended to be technically neutral, affording CEs & BAs flexibility in determining the best solutions and security controls for their environment. This agnostic approach takes into consideration that each CE & BA’s environment is unique. However, OCR investigations, resolution agreements, and settlements consistently reveal that CE & BAs remain challenged to understand how to apply the SR. In essence, it may be the delineation between knowledge of the SR and the ability to implement the SR. Repeat findings from OCR’s investigations further evidenced that CEs

& BAs SR risk analyses are insufficient and do not meet the demands of the regulatory mandate.

Reviewing OCR investigations, settlement agreements, and corrective action plans, it becomes evident that CEs & BAs need to conduct an accurate and thorough SR risk analysis. Understanding all of the information assets in a diverse healthcare entity is challenging, and as this research study shows, investment and leadership support are crucial. One pragmatic recommendation is to create cross-functional teams and to map out ePHI data touchpoints, and information flows. Data mapping would capture all the ingresses, egresses, locations, and touchpoints for all ePHI traversing the organization. Data mapping may help identify where ePHI is created, accessed, stored, and touched throughout an entire organization, including third parties. Information flow and data-mapping are no small tasks but would serve as an initial step toward the creation of a comprehensive, enterprise-wide SR risk analysis.

SR risk analysis is the foundation of an organization’s ePHI risk management approach toward meeting the SR regulatory mandates, but CEs & BAs continue to remain challenged to meet the comprehensiveness of OCR demands. The ability to create an accurate and thorough OCR quality risk analysis is the genesis toward understanding and creating effective strategies for the protection and privacy of ePHI data. Leveraging external SMEs to help in this endeavor may be necessary. One recommendation is that if external SMEs are considered, CEs & BAs need to vet the SME's abilities sufficiently. All SMEs are not created equal, and implementation competence and SR understanding may vary tremendously.

Reviewing an SME’s past SR implementations, interviewing previous clients, and inspecting breach responses and overall portfolios, may help identify key personnel. Finding an SME that fully understands the nuances of a genuine HIPAA SR (OCR quality) risk analysis is vital. Furthermore, it may be helpful to review prior (2012, 2015) OCR audit findings, as they highlight common improvement areas and help identify where improvements are required. It may be beneficial for privately held CEs & BAs to review U.S. Security and Exchange Commission (SEC) cybersecurity and resiliency disclosures, findings, observations, and guidance for publicly traded companies. These filings may offer insight into publicly-traded CEs & BAs’ cyber approach, controls, and how they addressed cyber risk factors while meeting the demands of regulatory mandates.

The quality and comprehensiveness of an initial SR risk analysis are critical, yet so is continual SR risk analysis updating, when environments are new, upgraded, and changed. Too often (based on OCR cases), CEs & BA’s approach toward updating SR risk analysis is insufficient and consists of an annual checklist, or a one and done task. Here again, board and executive leadership can help with mandates, guidance, and funding, based on the realization that an SR risk analysis is a constant and ever-evolving process, not just an annual event. It is recommended that security action line items and touchpoints are integrated into default project templates, maturity models, and timelines so that security is included in every step. SR risk analysis begins and ends with security. Too often, it appears that security is viewed as an after sight, checkbox, or speed bump to get over as quickly as possible during implementations, updates, overhauls, or routine processes.

Where SR compliance policies are in place, the expectation should be that they are monitored, adhered to, and violator(s) are sanctioned. The SR affords CEs & BAs the ability to apply sanctions to any individual (board member, owner, or employee) whose behavior(s) cause noncompliance or ePHI exposure (inadvertent or advertent) events. In order to convey this information in a non-threating manner, one recommendation is to bring in external legal counsel for HIPAA training. This counsel should specialize in HIPAA and provide training in the regulatory nature and power of HIPAA (privacy and security rule), focusing on personal culpability, individual liabilities, implications, and responsibility to adhere to compliance protocols. At times, information delivered via external sources versus internal sources, employees may tend to give the message more credence. Also, this external influence may help bolster an organization's compliance position and elevate the compliance awareness of all involved. In this manner, the message must be delivered in a non-threating manner, and with clarity, to all involved. No one is exempt from sanctions.

Having very clear sanction policies in place and reviewing these at a minimum of at least two times per year is recommended. Furthermore, there should be compliance scoreboards, graphically depicting compliance mishaps and events (anonymous in nature), but available for all staff and communicated monthly. It is common for organizations to post the number of days without physical injury publicly, so why not post information regarding SR compliance events. Most times, this information is heavily guarded and is not disseminated to the front lines, when it could be used as a comprehensive SR training and awareness tool. Compliance activity posting would be a powerful way to educate and elevate an organization's SR awareness and security culture, as it is based on real events inside an organization. Moreover, documenting proof of training and SR violation sanctions is a requirement under the SR.

Review of CC3 and CC5 - CC8 constructs showed that these areas are areas where CE & BAs may want to improve upon. It is not surprising that CC5 (SR funding) was number one on the participant response list. In 2019, a healthcare cybersecurity report from Healthcare Information and Management Systems Society (HIMSS) reported that over one quarter (26%) of healthcare organizations surveyed had no specific line item in their IT budget for cybersecurity. However, when asked explicitly about cybersecurity budget improvements over 2018, 72% of respondents indicated there was an increase (HIMSS, 2019). While it appears that some improvements in the healthcare organization's cybersecurity budgets have occurred, actual cybersecurity budgets are still small in comparison to the monies necessary for robust cybersecurity systems (HIMSS, 2019). One recommendation is for leadership to require separate security budget line items for existing and future system projects, including updates and enhancements. Owners and senior-level executives are encouraged to mandate that all existing and future IT projects, system updates, and improvements have separate compliance and cybersecurity budgetary line items. Specifically, compliance and security budgetary line items might help ensure that necessary funding (and focus) are baked into each and every step of a project (or retrofitted in the case of existing projects). This way, funding is planned for and not seen as an additional expense. This mandated budget integration would also alleviate dangerous assumptions that security efforts are already funded via existing budgetary line items, process workflows, and staff duties.

Management Support construct (CC3) showed that 44% of participants felt a lack of management support toward compliance with the SR. Owners and senior-level executives may still believe that cybersecurity is still just a department within IT. This luddite view only serves to perpetuate the lack of cybersecurity funding, leadership guidance, and board support. Lack of leadership support is not surprising, as confirmed by other research such as the Blackbook Market research annual healthcare IT and data security report. Blackbook Market Research LLC. (2018, 2019) reported that in 2018, (84%) and 2019 (79%) of hospitals were operating without a dedicated security executive. Compliance with today's cybersecurity and regulatory mandates demands an executive-level cybersecurity position in the board room and at the C-suite table. The cyber leadership role must be different and separate from that of a chief technology officer. One recommendation is that this position should report directly to the owners, board, or chief executive officer, and not the chief information or technology officer, due to potential conflicts of interest. CEs & BAs need to have senior cybersecurity leadership that creates, supports, and continually aligns their organization's cybersecurity strategies. Therefore, it is recommended that executive leadership is part of the interdepartmental cross-functional HIPAA security and compliance team. Too often, it seems, senior leadership delegates out this vital position, thinking of it as merely an IT issue; however, leadership guidance, support, and influence is critically needed at this level. An entire organization is impacted by ePHI, not just IT. Senior leadership may benefit from treating SR compliance with regulatory mandates as a corporate governance issue, one that demands engagement on behalf of the board and executives. This engagement may help empower the staff, aid in removing obstacles (political and personnel), and set the organization on a path toward actively managing the ever-evolving ePHI cyber compliance and risk landscape.

CC6 SR Technical Expertise (CC6) ranked fourth on the SRC survey. CC6 measured whether participants felt their organization had the level of technical expertise to comply with, implement, and monitor SR compliance. Only 39.5% of participants either strongly agreed or agreed. Over half of the SRC survey participants felt that their organization did not have the skill level or technical expertise to comply with, implement, and monitor SR compliance. Similar to CC5 (Funding), this is not surprising, as the cybersecurity profession is in extremely high demand (The Hill, 2019). One recommendation that may assist organizations right away and help identify candidates with the needed technical expertise is for CEs & BAs to partner up with National Security Agency (NSA), and National Centers of Academic Excellence (CAEs) accredited colleges and universities.

CAEs have cybersecurity programs that meet rigorous technical requirements, as developed by the NSA, Department of Homeland Security (DHS), and the Department of Defense (DoD) (Crumpler & Lewis, 2019). Top cybersecurity talent is in high demand, so it is not uncommon for cybersecurity undergraduates from CAE accredited universities to be hired before they graduate (Crumpler & Lewis, 2019). Therefore, it is recommended that CEs & BAs develop partnering, mentoring, and formalized internship, work-study, or job shadowing programs with accredited CAEs to help meet the demand for cybersecurity talent. Some CAE's have ongoing partnerships with others (retail, insurance, academic) organizations, yet healthcare appears to be tentative in integrating and leveraging this talent pool. CEs & BAs should provide a central point person to meet with CAEs, discuss needs and timing, and then collectively develop annual plans for internships, work-study, or job shadowing. This approach would create a skilled talent pipeline.

Organizational Focus (CC7) was ranked second by survey respondents, suggesting that an increase in organizational focus may increase SR compliance. Only 34.2% reported that Hardware and Systems (CC8), to monitor, audit, and secure ePHI were adequate and in place at their organization. Both of these issues may be related to funding issues (CC5); however, a focused commitment toward SR compliance and proper leadership direction appears to be needed. Existing or legacy hardware can be redistributed and deployed in such a way as to help meet SR compliance auditing and monitoring needs. One SR compliance area where CEs and & BAs appeared challenged was in confirming that existing security controls are actually working. Retooling legacy assets for logging, monitoring, and inspecting existing ePHI controls not only helps with financial constraints, but with SR compliance documentation mandates. This redeployment of legacy assets would provide artifacts of ongoing monitoring activities, should an event or OCR investigation ever occur. However, the reallocation of assets and resources takes organizational commitment, leadership influence, and a concentrated effort toward improving SR compliance posture (CC3). An increase in organizational focus does not always have to cost money, just a cultural shift in efforts and existing activities toward developing the security mindset and compliance culture required.

A prudent way to help drive security culture and organizational focus are for owners and senior-level executives to review their cyber insurance coverage with IT executives and managers. Matters such as these seem never to get distilled down to the front lines. A collective review of enterprise cyber coverage may be fruitful toward a mutual understanding of what liabilities are covered and, more importantly, what is not when breach events occur. Furthermore, insight may be gleaned by realizing what is not covered under one's breach insurance, as the cyber insurance market evolves continually. Sharing the contents of cyber and insurance policies with leadership, IT managers, and staff can only serve to promote healthy conversations about the current ePHI risk landscape, the organizational risk appetite, and actual (ePHI, financial and reputational) exposures of an organization. Moreover, dissemination of this information down to all levels may help engage leadership and provide a better understanding of their obligation to foster change in compliance practices, policies, and procedural behaviors.

Limitation and Future Studies

Limitations. Regulatory compliance research is complex, nuanced, and difficult to obtain (Parker & Nielsen, 2010). Many organizations want to keep compliance with regulatory statues private (Drahos, 2017b). Previous research in this area has also struggled with this, and results are only as good as the attestation comfort of the participant.

This research study's SRC survey was completely anonymous, helping induce participants to respond truthfully. Although anonymity afforded the participants greater comfort in which to respond with integrity, perhaps more case studies with a direct researcher to participant interaction may provide further insights. It should also be stated that all of these responses were based on an individual's perception of their organization's SR compliance posture. Although this research attempted to reach senior-level leadership, it was delivered in a completely anonymous fashion. As a result, participant’s compliance perceptions may be inaccurate based on their role and internal view of the organization, as well as the complete understanding of the organization’s actual compliance efforts. Furthermore, the Michigan-centric population response was expected, since this is the area in which the researcher resides and has numerous medical contacts.

Future Studies. The sample population included healthcare CEs & BAs operating within the U.S. This research study investigated the collective nature of CEs & BAs perceptions. However, Lisbon and Rice (2015), as well as Martin et al. (2015), purported that BAs (traditionally smaller organizations) may experience more difficulties in achieving and implementing SR compliance than CEs, which are traditionally larger organizations. Unfortunately, only 39 participants self-reported as BAs. This quantity of BA participants was not a large enough sample to perform advanced statistical analysis on the BA entity type alone.

As such, exploration and research endeavors that focus solely on BAs and their SR compliance challenges would be an area for future studies. It may be beneficial to improve this study by focusing on one industry type and one entity type (CEs or BAs). In this manner, SR compliance intricacies may be identified and may offer unique insight into the SR challenges specific industry, and entity types face.

Future studies could be centered on the best way to develop partnering, mentoring, and internship programs between CEs & BAs and accredited CAEs, and how to lessen the lack of cybersecurity talent. Development of an integrative framework that includes job shadowing, mentoring, and internships are one potential area worthy of investigating. Furthermore, future studies could focus on the efficacy of leveraging legacy equipment for the proactive monitoring and validation of security controls, another consistent weakness in OCR investigatory findings.

Summary

This study initially researched and identified a problem that exists with CEs & BAs compliance to the HIPAA SR regulatory strategy. The impact of which jeopardizes the security of highly sensitive and profoundly private patient ePHI. The study's introduction provided an in-depth overview of the problem and the challenges CEs & BAs face concerning SR compliance. The introduction aimed to provide a brief overview of how motives, characteristics, and capacities, regulator respect, as well as deterrence factors may play a significant role in the perception and likelihood of SR compliance posture in healthcare organizations.

Prior literature and regulatory studies detailed that scant research exists on HIPAA SR regulatory compliance. However, compliance research from other disciplines (i.e., environmental, and legal) helped develop the research question, constructs, and hypotheses, as well as creating a unique conceptual model for investigating the problem. The literature review highlighted several studies from differing fields of the regulatory compliance realm. Foundational studies that helped direct and frame this research were Parker and Nielsen (2010, 2011, 2017), Brady (2010), and Martin et al. (2015). Parker and Nielsen's work in compliance and regulatory strategy identified and developed the 14 dimensions of regulatory compliance. These dimensions were utilized and applied (with permission) toward understanding HIPAA SR compliance in CEs & BAs. The modification and utilization of these dimensions in the medical field provided this research study a unique view into the challenges CEs & BAs face, when complying to the HIPAA SR regulatory strategy.

The methodology chapter detailed a three-phased approach and highlighted the development of a survey-based instrument. By leveraging SMEs and a pilot study, the survey instrument was validated and deemed reliable to measure the constructs of motive (MT), characteristics and capacities (CC), regulator respect (RR), and deterrence factors (DT). The research design included the collection of data from CEs & BAs operating within the United States. Furthermore, empirical analysis of the participant's data included both descriptive statistics (frequency, mean) as well as multiple linear regression and Spearman's rho to address the research question and hypotheses adequately.

The results chapter provided the analysis and interpretation of findings from the participants (n=114) through assessment of motive, characteristics and capacities, regulator respect, and deterrence factors. The findings of this research study showed that there is a statistically significant positive correlation between PC1, MT, and CC, as well as a negative correlation between PC1 and DT. There was no correlation between PC1 and RR. Furthermore, MLR statistical analysis demonstrated that only CC was a statistically significant predictor of PC1.

The statistical significance between PC1 and CC was stronger than MT, RR, and DT combined. CC explained a majority of the variation in PC1, compared to the weak correlations of the other 3 IVs (MT, RR, and DT). MT, CC, and DT were all considered predictive of PC1, with CC having the strongest associative correlation, but two or more of the independent variables did not better predict PC1 than CC alone.

Finally, due to limited research devoted toward understanding the challenges CEs & BAs face, complying with the HIPAA SR, this research offered a new contribution to the current body of knowledge. This research developed a unique investigatory model to explore perceptions and the likelihood of compliance with SR regulatory strategy. This study and its implications may help drive future regulatory research and serve to provide organizations with insight(s) on how to address compliance toward the SR regulatory strategy pragmatically, with the ultimate goal being of increasing security and safeguarding ePHI.

Appendices

Appendix A:

Martin et al. (2015), HIPAA Security Rule Compliance Theoretical Framework.

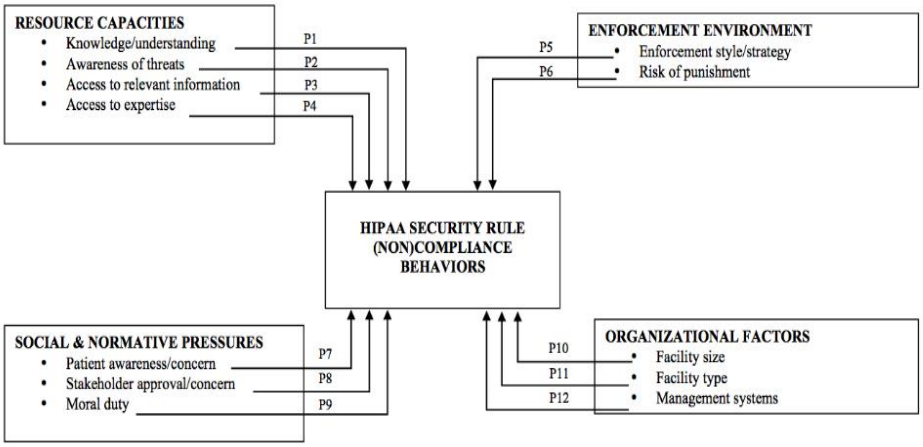


Figure A1. Martin et al. (2015) HIPAA security rule compliance in small healthcare facilities: a theoretical framework. (Provided with permission)(Martin et al., 2015).

Appendix B:

Parker and Nielsen (2011), Holistic and Plural Model of Business Compliance.

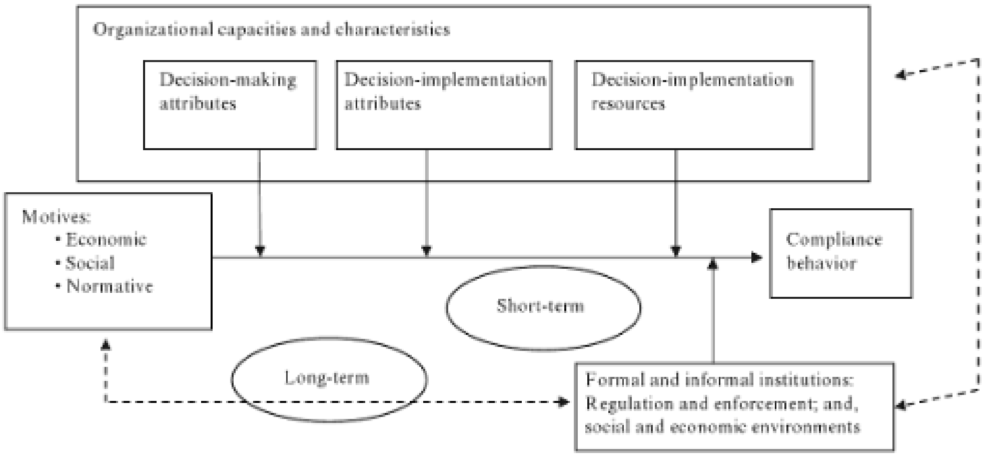
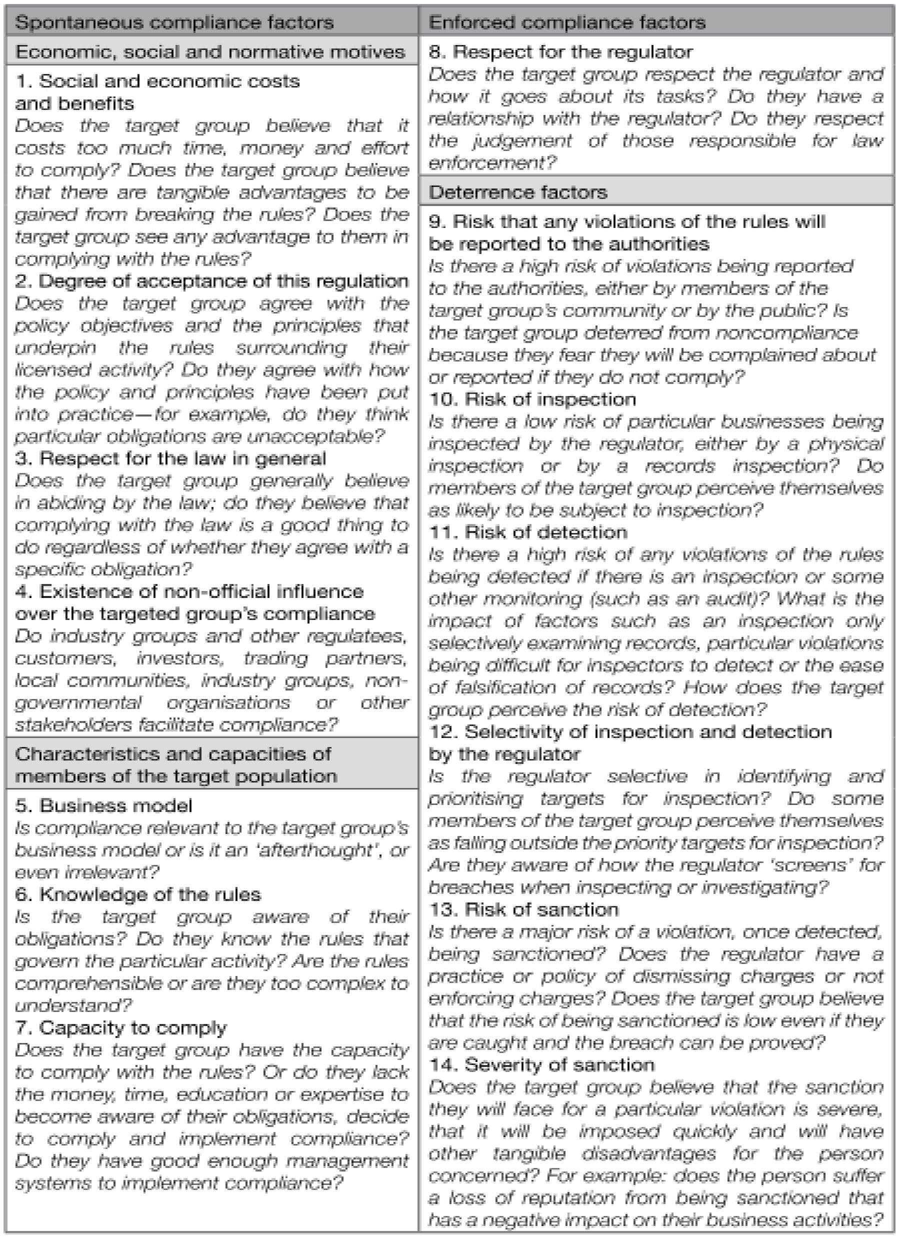

Organizational capacities and characteristics
Decision-making attributes
Decision-implementation attributes
Decision-implementation resources
Motives:
• Economic
• Social
• Normative
Compliance behavior
Short-term
Long-term
Formal and informal institutions: Regulation and enforcement; and, social and economic environments

Figure B1. Parker and Nielsen (2011), Holistic and plural model of business compliance. Provided with permission (Parker & Nielsen, 2011).

Appendix C:

Parker and Nielsen (2017) 14 Compliance Dimensions

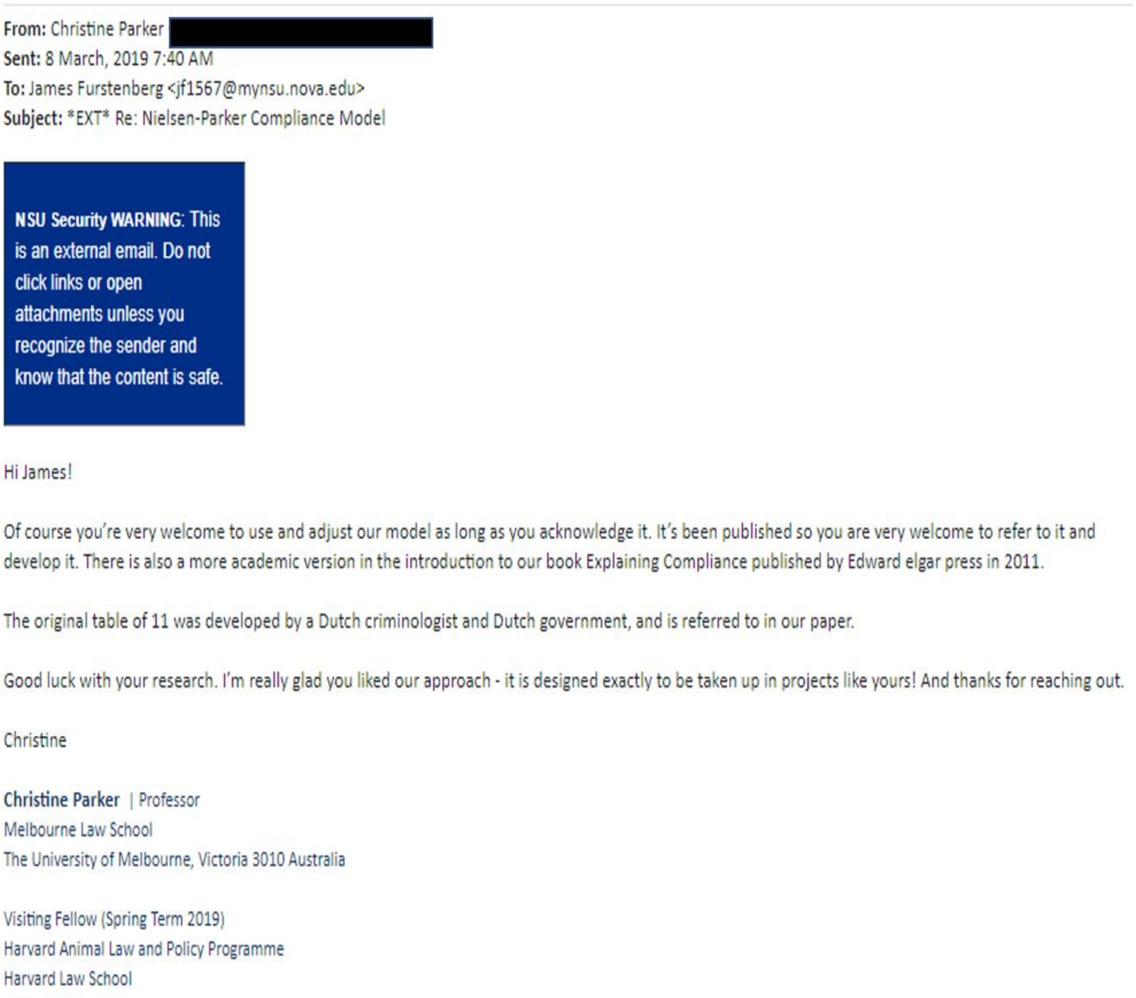


Spontaneous compliance factors	Enforced compliance factors
Economic, social and normative motives **1. Social and economic costs and benefits** *Does the target group believe that it costs too much time, money and effort to comply? Does the target group believe that there are tangible advantages to be gained from breaking the rules? Does the target group see any advantage to them in complying with the rules?* **2. Degree of acceptance of this regulation** *Does the target group agree with the policy objectives and the principles that underpin the rules surrounding their licensed activity? Do they agree with how the policy and principles have been put into practice—for example, do they think particular obligations are unacceptable?* **3. Respect for the law in general** *Does the target group generally believe in abiding by the law; do they believe that complying with the law is a good thing to do regardless of whether they agree with a specific obligation?* **4. Existence of non-official influence over the targeted group's compliance** *Do industry groups and other regulatees, customers, investors, trading partners, local communities, industry groups, non-governmental organisations or other stakeholders facilitate compliance?* **Characteristics and capacities of members of the target population** **5. Business model** *Is compliance relevant to the target group's business model or is it an 'afterthought', or even irrelevant?* **6. Knowledge of the rules** *Is the target group aware of their obligations? Do they know the rules that govern the particular activity? Are the rules comprehensible or are they too complex to understand?* **7. Capacity to comply** *Does the target group have the capacity to comply with the rules? Or do they lack the money, time, education or expertise to become aware of their obligations, decide to comply and implement compliance? Do they have good enough management systems to implement compliance?*	**8. Respect for the regulator** *Does the target group respect the regulator and how it goes about its tasks? Do they have a relationship with the regulator? Do they respect the judgement of those responsible for law enforcement?* **Deterrence factors** **9. Risk that any violations of the rules will be reported to the authorities** *Is there a high risk of violations being reported to the authorities, either by members of the target group's community or by the public? Is the target group deterred from noncompliance because they fear they will be complained about or reported if they do not comply?* **10. Risk of inspection** *Is there a low risk of particular businesses being inspected by the regulator, either by a physical inspection or by a records inspection? Do members of the target group perceive themselves as likely to be subject to inspection?* **11. Risk of detection** *Is there a high risk of any violations of the rules being detected if there is an inspection or some other monitoring (such as an audit)? What is the impact of factors such as an inspection only selectively examining records, particular violations being difficult for inspectors to detect or the ease of falsification of records? How does the target group perceive the risk of detection?* **12. Selectivity of inspection and detection by the regulator** *Is the regulator selective in identifying and prioritising targets for inspection? Do some members of the target group perceive themselves as falling outside the priority targets for inspection? Are they aware of how the regulator 'screens' for breaches when inspecting or investigating?* **13. Risk of sanction** *Is there a major risk of a violation, once detected, being sanctioned? Does the regulator have a practice or policy of dismissing charges or not enforcing charges? Does the target group believe that the risk of being sanctioned is low even if they are caught and the breach can be proved?* **14. Severity of sanction** *Does the target group believe that the sanction they will face for a particular violation is severe, that it will be imposed quickly and will have other tangible disadvantages for the person concerned? For example: does the person suffer a loss of reputation from being sanctioned that has a negative impact on their business activities?*

Figure C1. Parker & Nielsen (2017) 14 Compliance Dimensions (Provided with permission).

Appendix D:

Dr. Christine Parker Permission.



From: Christine Parker [redacted]
Sent: 8 March, 2019 7:40 AM
To: James Furstenberg <jf1567@mynsu.nova.edu>
Subject: *EXT* Re: Nielsen-Parker Compliance Model

NSU Security WARNING: This is an external email. Do not click links or open attachments unless you recognize the sender and know that the content is safe.

Hi James!

Of course you're very welcome to use and adjust our model as long as you acknowledge it. It's been published so you are very welcome to refer to it and develop it. There is also a more academic version in the introduction to our book Explaining Compliance published by Edward elgar press in 2011.

The original table of 11 was developed by a Dutch criminologist and Dutch government, and is referred to in our paper.

Good luck with your research. I'm really glad you liked our approach - it is designed exactly to be taken up in projects like yours! And thanks for reaching out.

Christine

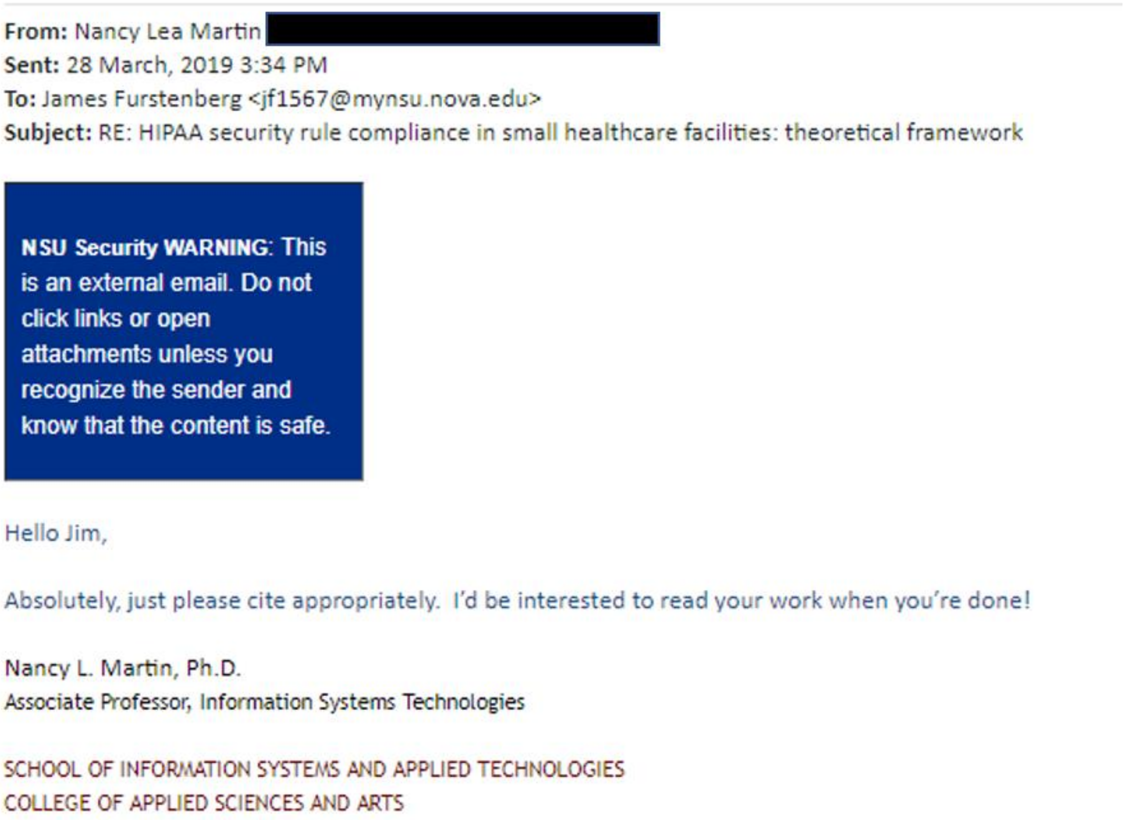
Christine Parker | Professor
Melbourne Law School
The University of Melbourne, Victoria 3010 Australia

Visiting Fellow (Spring Term 2019)
Harvard Animal Law and Policy Programme
Harvard Law School

Figure D1. Dr. Christine Parker Permission.

Appendix E:

Dr. Nancy Martin Permission.



From: Nancy Lea Martin [redacted]
Sent: 28 March, 2019 3:34 PM
To: James Furstenberg <jf1567@mynsu.nova.edu>
Subject: RE: HIPAA security rule compliance in small healthcare facilities: theoretical framework

NSU Security WARNING: This is an external email. Do not click links or open attachments unless you recognize the sender and know that the content is safe.

Hello Jim,

Absolutely, just please cite appropriately. I'd be interested to read your work when you're done!

Nancy L. Martin, Ph.D.
Associate Professor, Information Systems Technologies

SCHOOL OF INFORMATION SYSTEMS AND APPLIED TECHNOLOGIES
COLLEGE OF APPLIED SCIENCES AND ARTS

Figure E1. Dr. Nancy Martin Permission.

Appendix F:

Table F1

Motive Constructs, Questions, and References

Construct	Survey Question	References
MT1	Complying with the SR costs too much time and money.	Bulgurcu, B., Cavusoglu, H., & Izak, B. (2010)
MT2	Superficial adoption of the SR provides substantial advantages.	Zhang, N., & Zhang, N. (2018)
MT3	Complying with the SR aligns with our organization's mission(s) and goal(s).	(X. Chen, Wu, Chen, & Teng, 2018)
MT4	Our organization agrees with the SR regulatory strategy, its policy objectives, and the principles that underpin it.	Nielsen, V., & Parker, C. (2012)
MT5	Do you agree with how the SR regulatory policy has been put into practice at your organization?	Huang, H., & Liu, C.-L. (2018)
MT6	The SR compliance obligations and requirements are acceptable.	Bulgurcu, B., Cavusoglu, H., & Izak, B. (2010)
MT7	Compliance with the SR is beneficial despite the specific safeguards and obligations.	Bulgurcu, B., Cavusoglu, H., & Izak, B. (2010)
MT8	Adoption of SR compliance is influenced by industry groups, regulators, customers, investors trading partners communities, non-governmental organizations, or any other stakeholders.	X. Chen, Wu, Chen, & Teng, 2018)

Appendix F: continued

Table F2

Characteristic & Capacities Constructs, Questions and References

Construct	Survey Question	References
CC1	SR compliance is relevant to our organization’s business model.	Appari, Johnson, & Anthony (2009)
CC2	Our organization is fully aware of the SR standards and obligations.	Angst, C. M., Block, E. S., D ’Arcy, J., & Kelley, K. (2017)
CC3	Our organization knows the SR safeguards and implementation specifications that govern compliance requirements.	Gaia, Wang, Basile, Sanders, & Murry (2018)
CC4	The SR is too complex to comply with or implement fully.	Nielsen, V., & Parker, C. (2012)
CC5	Our organization provides adequate funding for SR compliance and implementation of the SR.	Gaia, Wang, Basile, Sanders, & Murray (2018)
CC6	Our organization has the level of technical expertise to comply with, implement, and monitor SR compliance.	Gaia, Wang, Basile, Sanders, & Murray (2018)
CC7	There is enough time devoted to implementing and monitoring SR compliance.	Nielsen, V., & Parker, C. (2012)
CC8	There are enough management systems and management support to implement and monitor SR compliance.	Brady, J. W. (2010)

Appendix F: continued

Table F3

Regulator Respect Constructs, Questions, and References

Construct	Survey Question	References
RR1	Our organization respects how the Office for Civil Rights educates and supports organizations about SR compliance.	Drahos, P., & Krygier, M. (2017)
RR2	Our organization respects how the Office for Civil Rights enforces SR compliance.	Drahos, P., & Krygier, M. (2017)
RR3	Our organization has a strong relationship with the Office for Civil Rights auditor(s) and regulator(s).	Parker, C., & Nielsen, V. (2017)
RR4	Our organization respects the Office for Civil Rights judgments, civil monetary fines, and resolution agreements relating to SR enforcement.	Murphy, K., Tyler, T. R., & Curtis, A. (2009)

Appendix F: continued

Table F4

Deterrence Factor Constructs, Questions, and References

Construct	Survey Question	References
DT1	There a high risk of violations being reported to the authorities either by members of the organization, community or by the public.	Gaia, Wang, Basile, Sanders, & Murray (2018)
DT2	Compliance with the SR is due to fear of violations, complaints, or reports.	Nielsen, V., & Parker, C. (2012)
DT3	Our organization is at a lower risk of being inspected by the Office for Civil Rights for SR violations.	Gaia, Wang, Basile, Sanders, & Murray (2018)
DT4	The likelihood that our organization will be subjected to HIPAA inspection due to an SR breach or violation is very low.	Nielsen, V., & Parker, C. (2012).
DT5	Monitoring, such as an audit, would not reveal any SR violations at our organization.	Gaia, Wang, Basile, Sanders, & Murray (2018)
DT6	The integrity of our organization SR violation records is such that it would be difficult for inspectors to detect or a trace falsification of records.	Martin, N. L., Imboden, T., & Green, D. T. (2015)
DT7	The risk for an SR violation being detected is low	Nielsen, V., & Parker, C. (2012)

Appendix F: continued

Table F4 (continued)

Deterrence Factor Constructs, Questions, and References (continued)

Construct	Survey Question	References
DT8	The Office for Civil Rights is selective in identifying and prioritizing targets for inspection.	Gaia, Wang, Basile, Sanders, & Murray (2018)
DT9	Our organization falls outside of the priority targets for SR compliance inspection.	Barlow, J. B., Dennis, A. R., Warkentin, M., & Ormond, D. (2018)
DT10	Our organization understands how the Office for Civil Rights screens for breaches when inspecting or investigating SR compliance issues.	Nielsen, V., & Parker, C. (2012
DT11	If an SR compliance violation is detected, there is a significant risk of enforcement actions and sanctioning.	Nielsen, V., & Parker, C. (2012)
DT12	The Office for Civil rights has a practice of dismissing charges or not enforcing charges.	Gaia, Wang, Basile, Sanders, & Murray (2018)
DT13	The risk of being sanctioned is low, even if being caught in a breach can be proved.	Nielsen, V., & Parker, C. (2012).
DT14	Violations for SR non-compliance will be imposed quickly and will have consequences.	Gaia, Wang, Basile, Sanders, & Murray (2018)
DT15	SR violations and civil monetary penalties would negatively impact our organization.	X. Chen, Wu, Chen, & Teng (2018)

Appendix F: continued

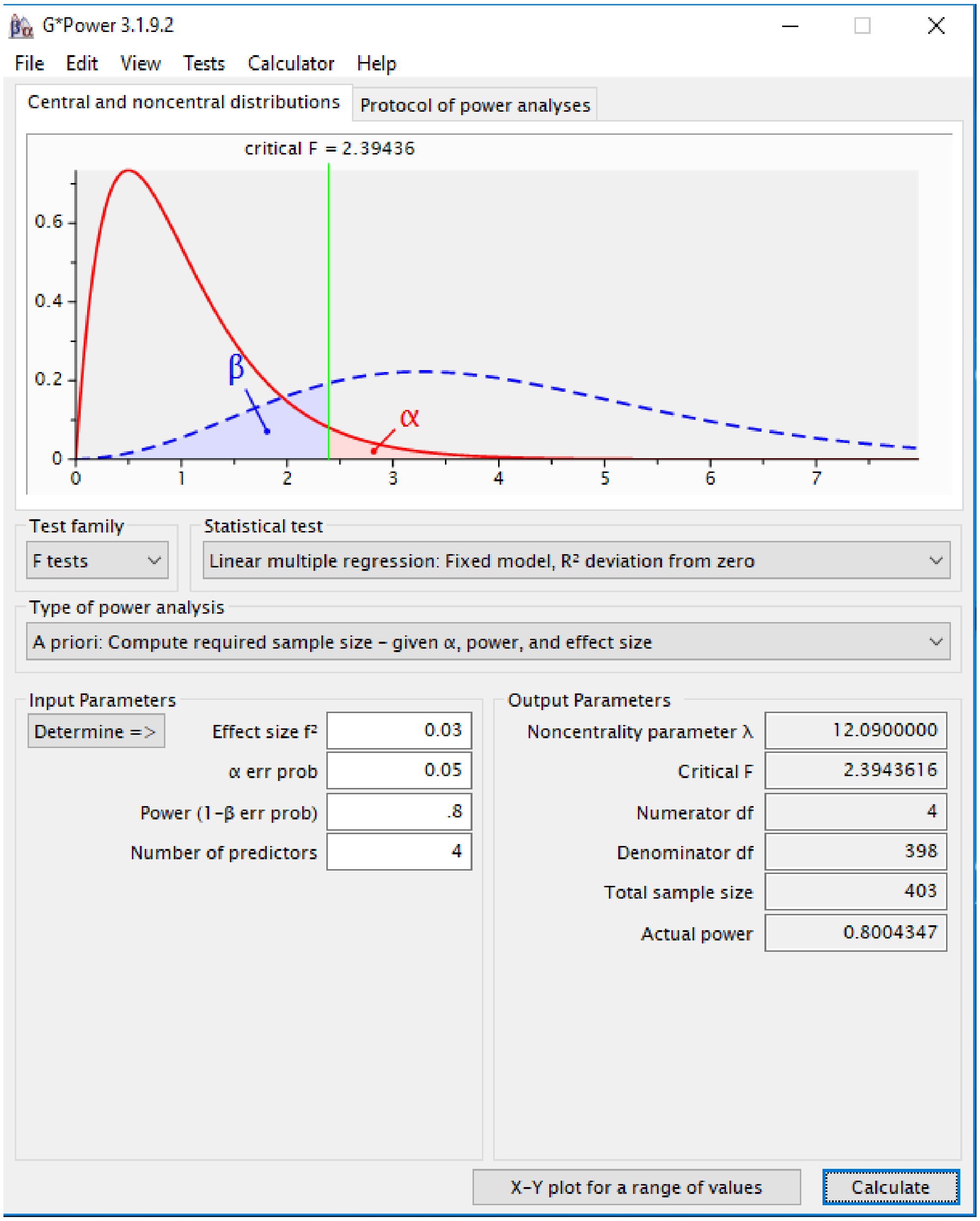
Table F5

Perceived Compliance Likelihood Construct, Question, and References

Construct	Survey Question	References
PC1	Our organization is fully compliant with SR regulatory standards, safeguards, and implementation specifications.	Gaia, Wang, Basile, Sanders, & Murray (2018)

Appendix G:

*G*Power Settings and Results to Determine Effect Size for H1-H4*



Test family: F tests

Statistical test: Linear multiple regression: Fixed model, R² deviation from zero

Type of power analysis: A priori: Compute required sample size – given α, power, and effect size

Input Parameters

Effect size f²	0.03
α err prob	0.05
Power (1-β err prob)	.8
Number of predictors	4

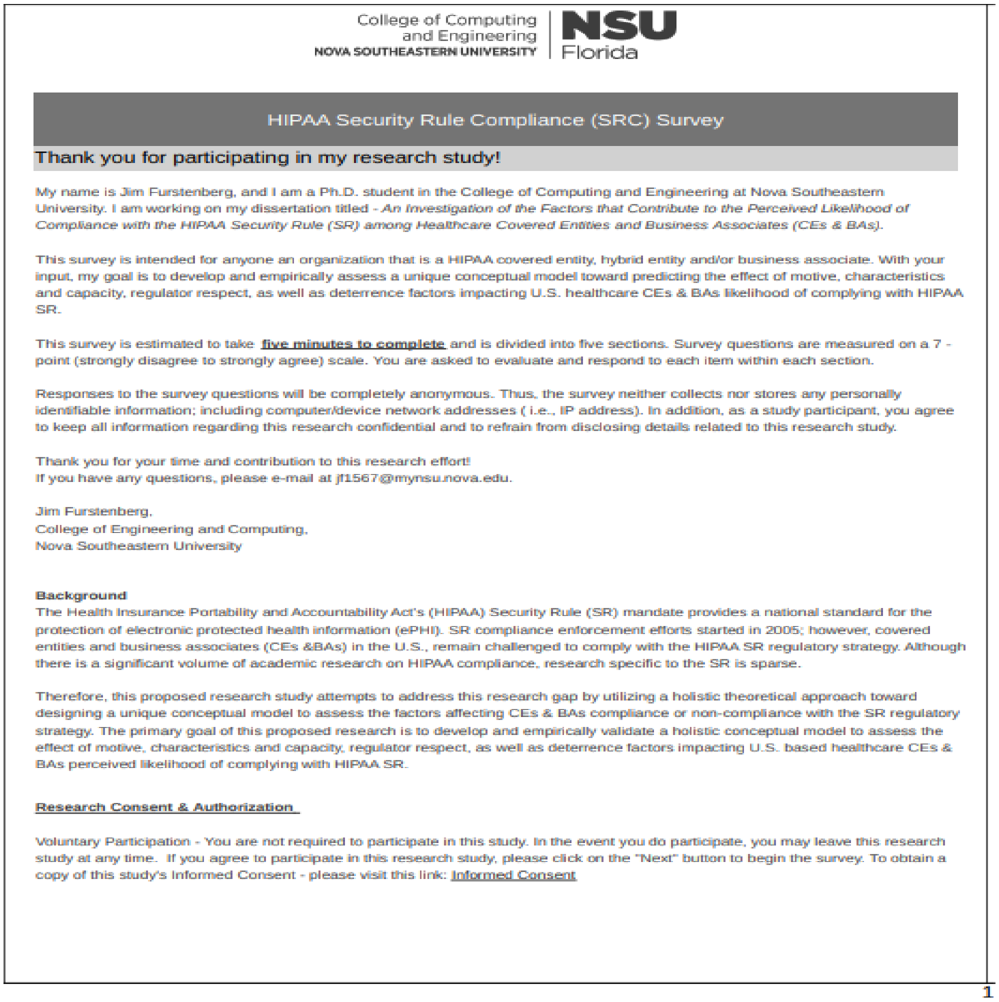
Output Parameters

Noncentrality parameter λ	12.0900000
Critical F	2.3943616
Numerator df	4
Denominator df	398
Total sample size	403
Actual power	0.8004347

Figure G1. G*Power Settings and Results to Determine Effect Size for H1-H4

Appendix H:

Final SRC Survey Instrument



College of Computing
and Engineering
NOVA SOUTHEASTERN UNIVERSITY | NSU Florida

HIPAA Security Rule Compliance (SRC) Survey

Thank you for participating in my research study!

My name is Jim Furstenberg, and I am a Ph.D. student in the College of Computing and Engineering at Nova Southeastern University. I am working on my dissertation titled - *An Investigation of the Factors that Contribute to the Perceived Likelihood of Compliance with the HIPAA Security Rule (SR) among Healthcare Covered Entities and Business Associates (CEs & BAs).*

This survey is intended for anyone an organization that is a HIPAA covered entity, hybrid entity and/or business associate. With your input, my goal is to develop and empirically assess a unique conceptual model toward predicting the effect of motive, characteristics and capacity, regulator respect, as well as deterrence factors impacting U.S. healthcare CEs & BAs likelihood of complying with HIPAA SR.

This survey is estimated to take **five minutes to complete** and is divided into five sections. Survey questions are measured on a 7 - point (strongly disagree to strongly agree) scale. You are asked to evaluate and respond to each item within each section.

Responses to the survey questions will be completely anonymous. Thus, the survey neither collects nor stores any personally identifiable information; including computer/device network addresses (i.e., IP address). In addition, as a study participant, you agree to keep all information regarding this research confidential and to refrain from disclosing details related to this research study.

Thank you for your time and contribution to this research effort!
If you have any questions, please e-mail at jf1567@mynsu.nova.edu.

Jim Furstenberg,
College of Engineering and Computing,
Nova Southeastern University

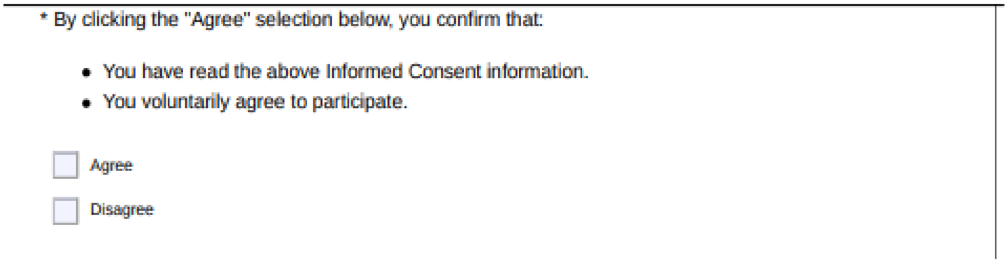
Background
The Health Insurance Portability and Accountability Act's (HIPAA) Security Rule (SR) mandate provides a national standard for the protection of electronic protected health information (ePHI). SR compliance enforcement efforts started in 2005; however, covered entities and business associates (CEs &BAs) in the U.S., remain challenged to comply with the HIPAA SR regulatory strategy. Although there is a significant volume of academic research on HIPAA compliance, research specific to the SR is sparse.

Therefore, this proposed research study attempts to address this research gap by utilizing a holistic theoretical approach toward designing a unique conceptual model to assess the factors affecting CEs & BAs compliance or non-compliance with the SR regulatory strategy. The primary goal of this proposed research is to develop and empirically validate a holistic conceptual model to assess the effect of motive, characteristics and capacity, regulator respect, as well as deterrence factors impacting U.S. based healthcare CEs & BAs perceived likelihood of complying with HIPAA SR.

Research Consent & Authorization

Voluntary Participation - You are not required to participate in this study. In the event you do participate, you may leave this research study at any time. If you agree to participate in this research study, please click on the "Next" button to begin the survey. To obtain a copy of this study's Informed Consent - please visit this link: Informed Consent

1



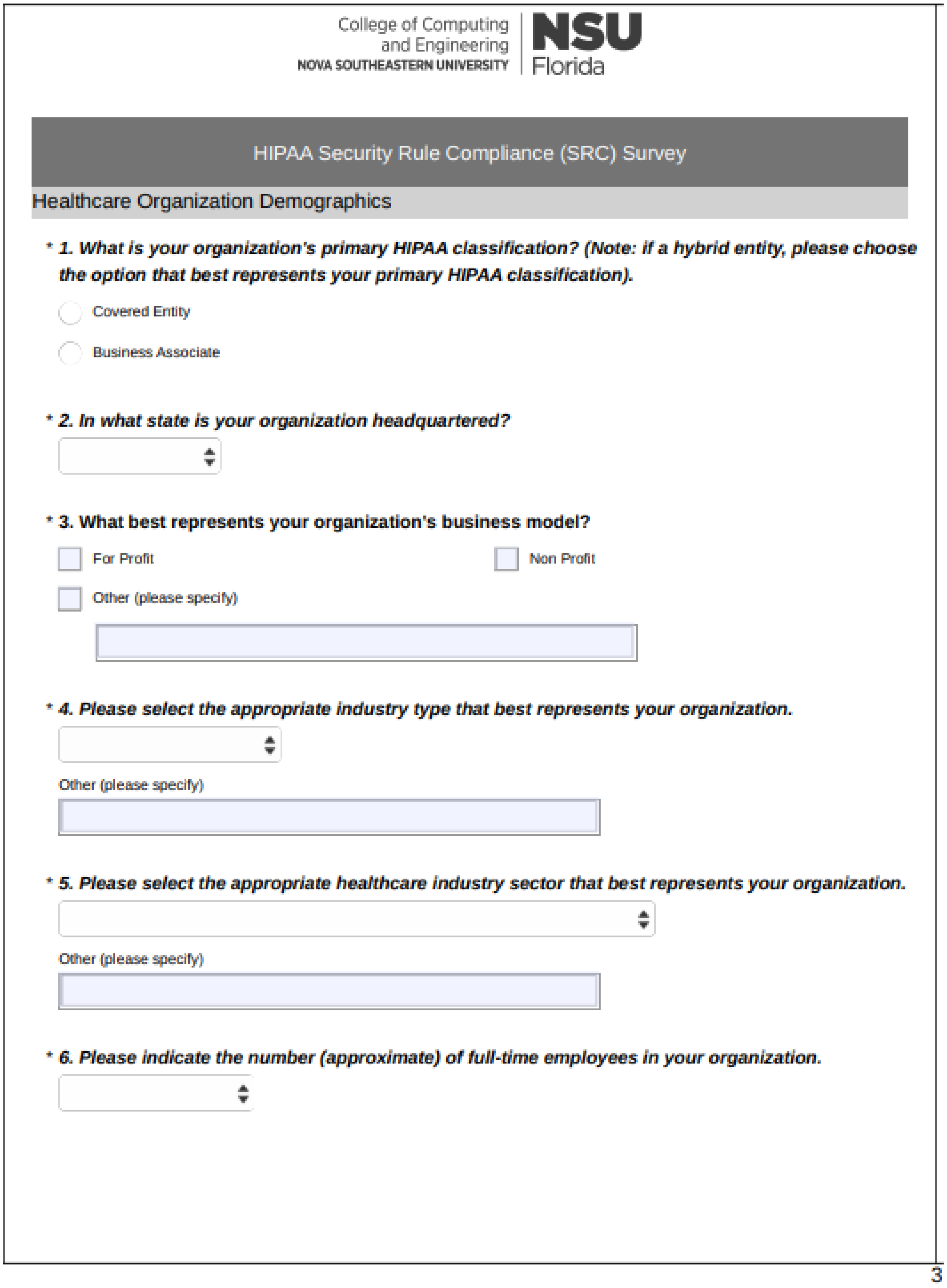
* By clicking the "Agree" selection below, you confirm that:

- You have read the above Informed Consent information.
- You voluntarily agree to participate.

□ Agree

□ Disagree

Appendix H continued:



College of Computing
and Engineering
NOVA SOUTHEASTERN UNIVERSITY

NSU
Florida

HIPAA Security Rule Compliance (SRC) Survey

Healthcare Organization Demographics

* ***1. What is your organization's primary HIPAA classification? (Note: if a hybrid entity, please choose the option that best represents your primary HIPAA classification).***

○ Covered Entity

○ Business Associate

* ***2. In what state is your organization headquartered?***

* **3. What best represents your organization's business model?**

□ For Profit　　□ Non Profit

□ Other (please specify)

* ***4. Please select the appropriate industry type that best represents your organization.***

Other (please specify)

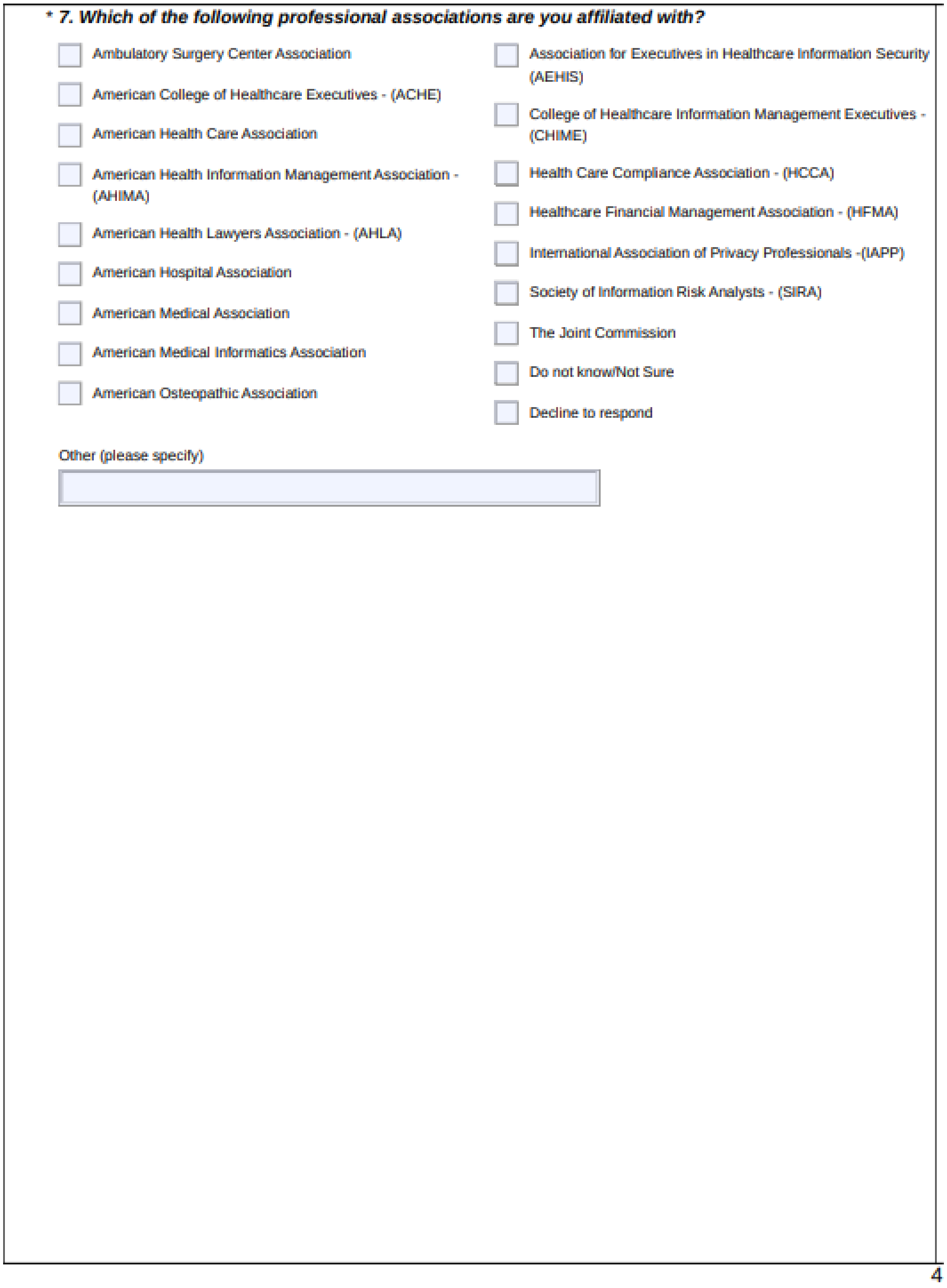
* ***5. Please select the appropriate healthcare industry sector that best represents your organization.***

Other (please specify)

* ***6. Please indicate the number (approximate) of full-time employees in your organization.***

3

Appendix H continued:



*** 7. Which of the following professional associations are you affiliated with?**

□ Ambulatory Surgery Center Association

□ American College of Healthcare Executives - (ACHE)

□ American Health Care Association

□ American Health Information Management Association - (AHIMA)

□ American Health Lawyers Association - (AHLA)

□ American Hospital Association

□ American Medical Association

□ American Medical Informatics Association

□ American Osteopathic Association

□ Association for Executives in Healthcare Information Security (AEHIS)

□ College of Healthcare Information Management Executives - (CHIME)

□ Health Care Compliance Association - (HCCA)

□ Healthcare Financial Management Association - (HFMA)

□ International Association of Privacy Professionals -(IAPP)

□ Society of Information Risk Analysts - (SIRA)

□ The Joint Commission

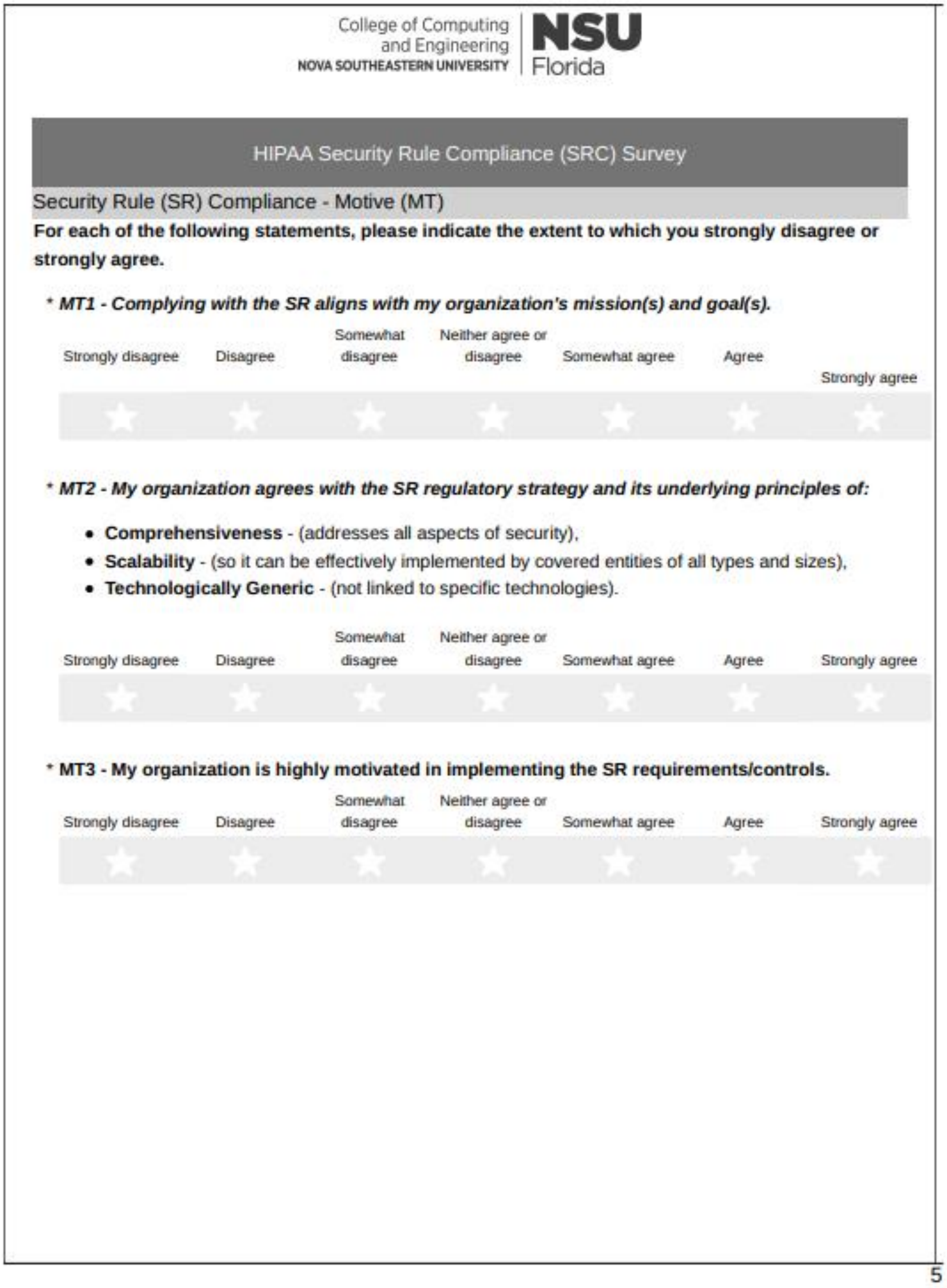
□ Do not know/Not Sure

□ Decline to respond

Other (please specify)

4

Appendix H continued:



College of Computing
and Engineering
NOVA SOUTHEASTERN UNIVERSITY
NSU
Florida

HIPAA Security Rule Compliance (SRC) Survey

Security Rule (SR) Compliance - Motive (MT)

For each of the following statements, please indicate the extent to which you strongly disagree or strongly agree.

* ***MT1 - Complying with the SR aligns with my organization's mission(s) and goal(s).***

Strongly disagree	Disagree	Somewhat disagree	Neither agree or disagree	Somewhat agree	Agree	Strongly agree
★	★	★	★	★	★	★

* ***MT2 - My organization agrees with the SR regulatory strategy and its underlying principles of:***

- **Comprehensiveness** - (addresses all aspects of security),
- **Scalability** - (so it can be effectively implemented by covered entities of all types and sizes),
- **Technologically Generic** - (not linked to specific technologies).

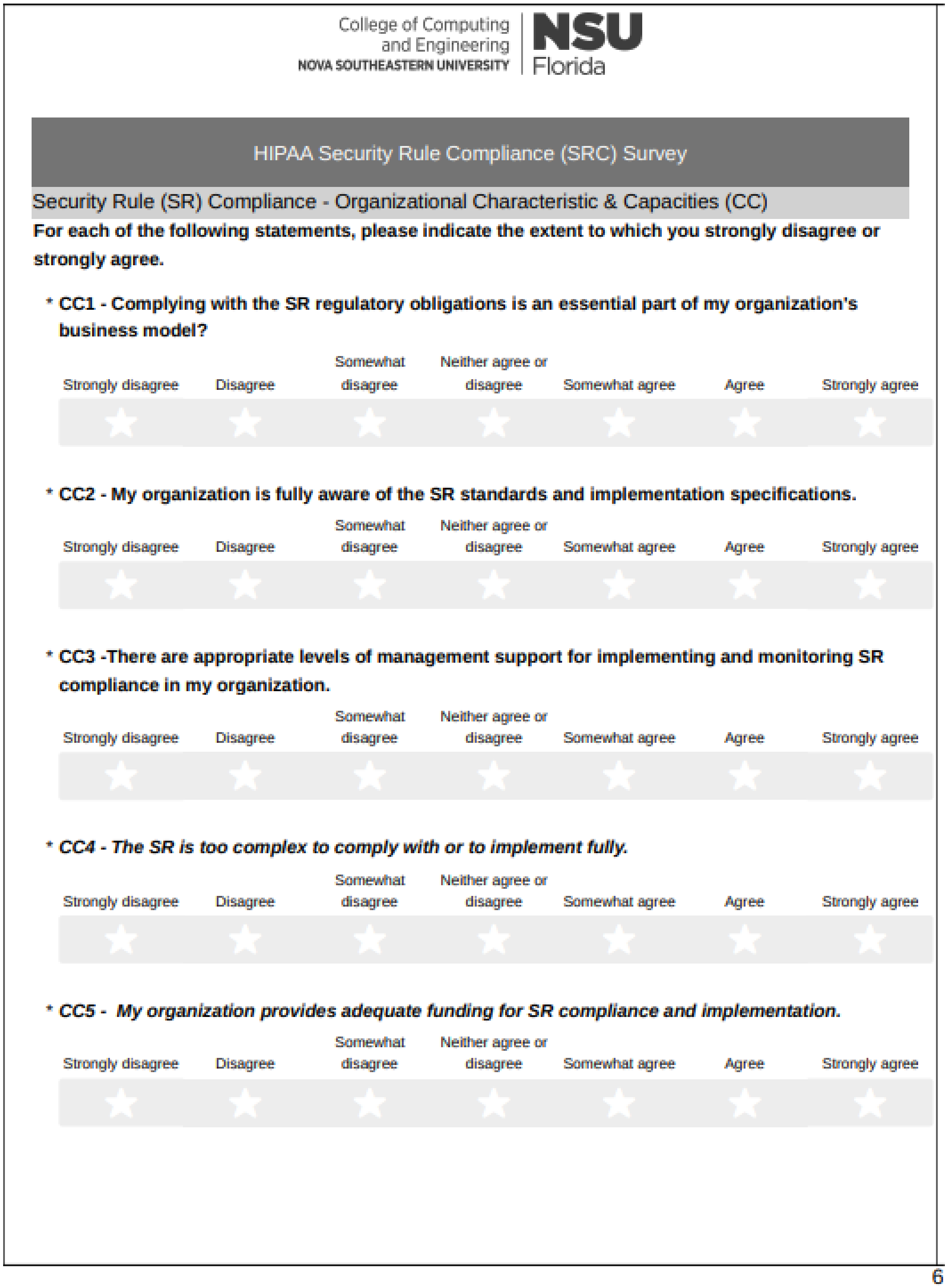
Strongly disagree	Disagree	Somewhat disagree	Neither agree or disagree	Somewhat agree	Agree	Strongly agree
★	★	★	★	★	★	★

* **MT3 - My organization is highly motivated in implementing the SR requirements/controls.**

Strongly disagree	Disagree	Somewhat disagree	Neither agree or disagree	Somewhat agree	Agree	Strongly agree
★	★	★	★	★	★	★

5

Appendix H continued:



College of Computing
and Engineering
NOVA SOUTHEASTERN UNIVERSITY

NSU
Florida

HIPAA Security Rule Compliance (SRC) Survey

Security Rule (SR) Compliance - Organizational Characteristic & Capacities (CC)

For each of the following statements, please indicate the extent to which you strongly disagree or strongly agree.

* **CC1 - Complying with the SR regulatory obligations is an essential part of my organization's business model?**

Strongly disagree	Disagree	Somewhat disagree	Neither agree or disagree	Somewhat agree	Agree	Strongly agree
☆	☆	☆	☆	☆	☆	☆

* **CC2 - My organization is fully aware of the SR standards and implementation specifications.**

Strongly disagree	Disagree	Somewhat disagree	Neither agree or disagree	Somewhat agree	Agree	Strongly agree
☆	☆	☆	☆	☆	☆	☆

* **CC3 -There are appropriate levels of management support for implementing and monitoring SR compliance in my organization.**

Strongly disagree	Disagree	Somewhat disagree	Neither agree or disagree	Somewhat agree	Agree	Strongly agree
☆	☆	☆	☆	☆	☆	☆

* ***CC4 - The SR is too complex to comply with or to implement fully.***

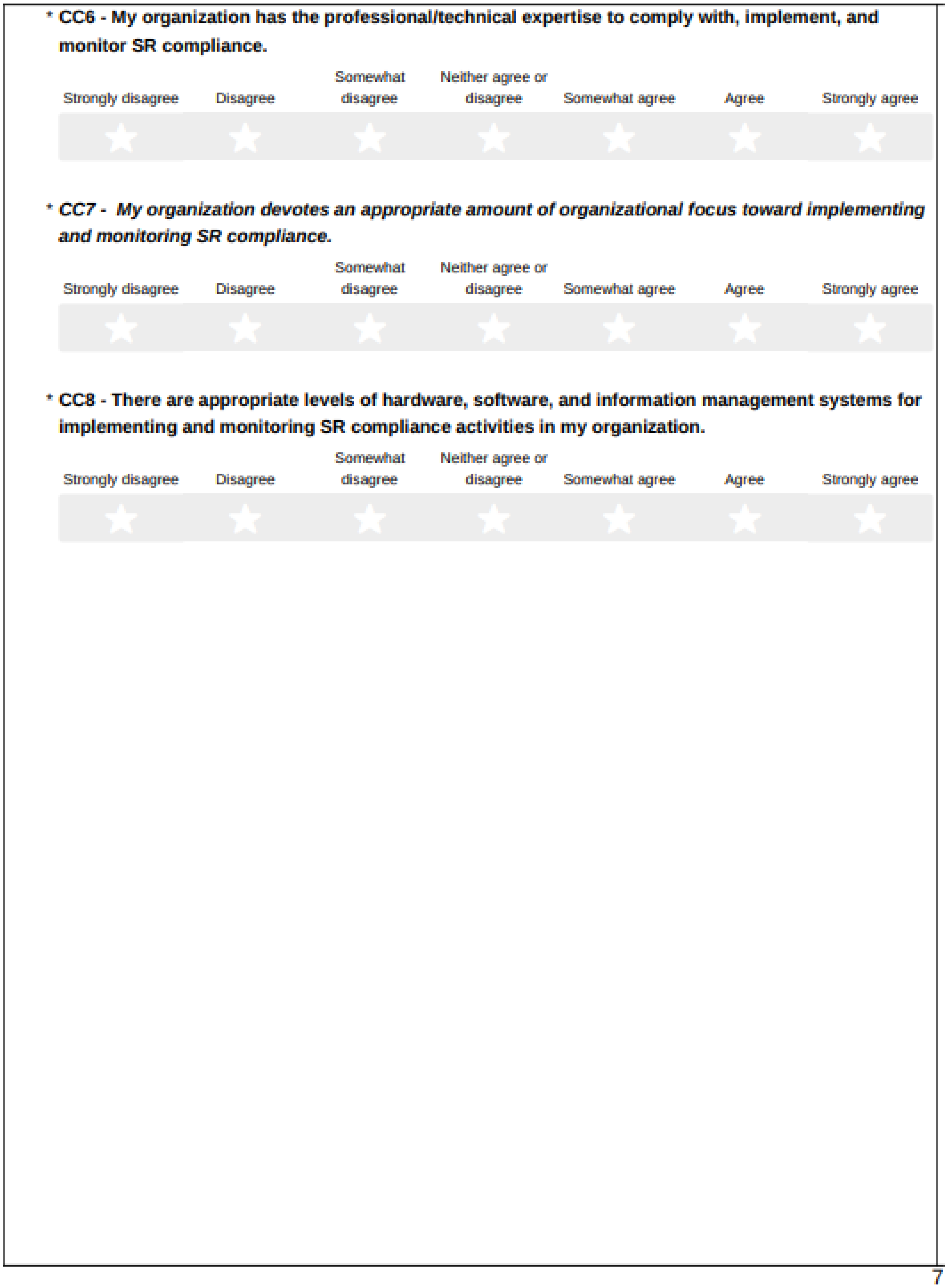
Strongly disagree	Disagree	Somewhat disagree	Neither agree or disagree	Somewhat agree	Agree	Strongly agree
☆	☆	☆	☆	☆	☆	☆

* ***CC5 - My organization provides adequate funding for SR compliance and implementation.***

Strongly disagree	Disagree	Somewhat disagree	Neither agree or disagree	Somewhat agree	Agree	Strongly agree
☆	☆	☆	☆	☆	☆	☆

6

Appendix H continued:



* **CC6 - My organization has the professional/technical expertise to comply with, implement, and monitor SR compliance.**

Strongly disagree	Disagree	Somewhat disagree	Neither agree or disagree	Somewhat agree	Agree	Strongly agree
☆	☆	☆	☆	☆	☆	☆

* ***CC7 - My organization devotes an appropriate amount of organizational focus toward implementing and monitoring SR compliance.***

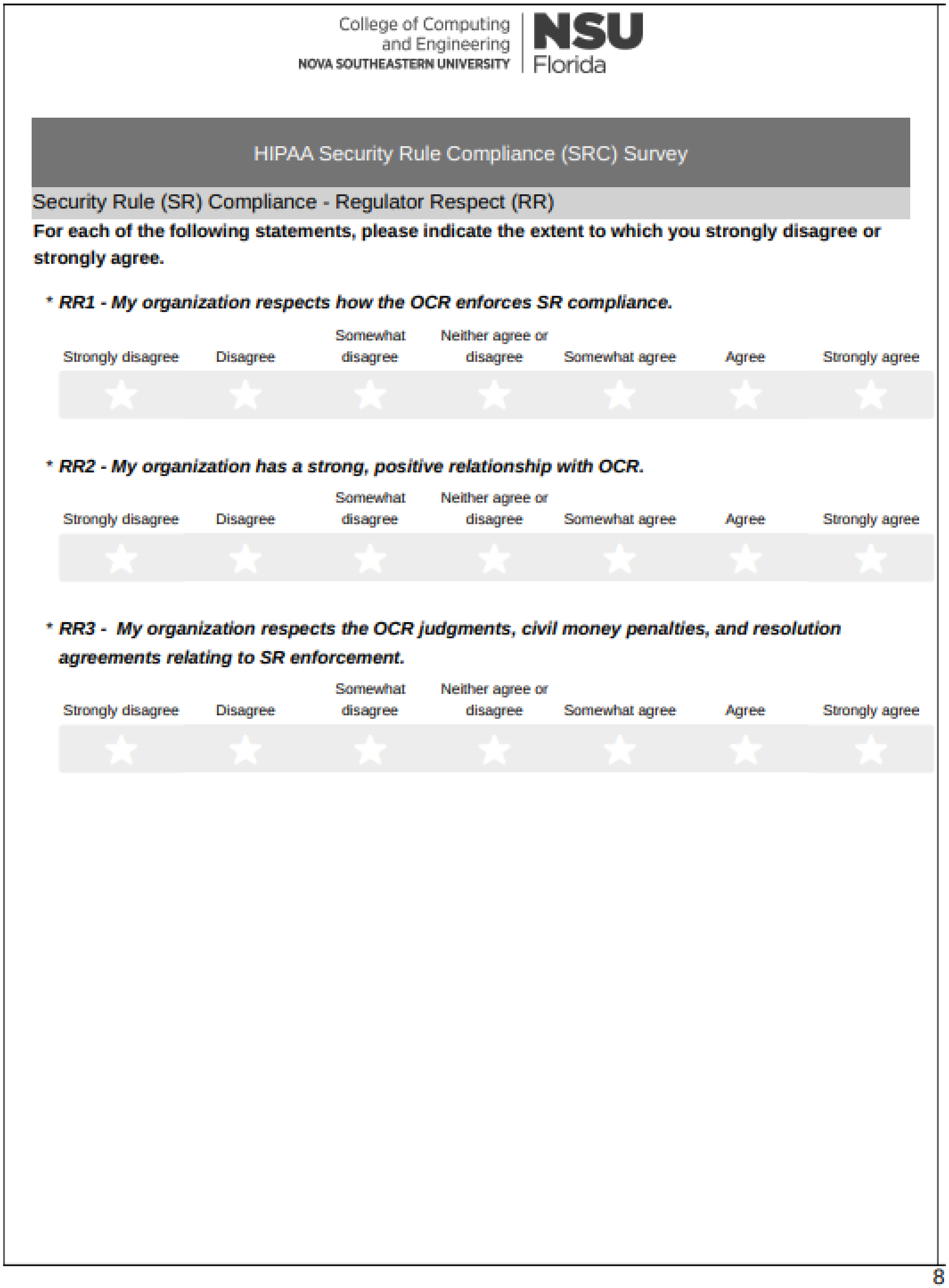
Strongly disagree	Disagree	Somewhat disagree	Neither agree or disagree	Somewhat agree	Agree	Strongly agree
☆	☆	☆	☆	☆	☆	☆

* **CC8 - There are appropriate levels of hardware, software, and information management systems for implementing and monitoring SR compliance activities in my organization.**

Strongly disagree	Disagree	Somewhat disagree	Neither agree or disagree	Somewhat agree	Agree	Strongly agree
☆	☆	☆	☆	☆	☆	☆

7

Appendix H continued:



College of Computing and Engineering
NOVA SOUTHEASTERN UNIVERSITY | NSU Florida

HIPAA Security Rule Compliance (SRC) Survey

Security Rule (SR) Compliance - Regulator Respect (RR)

For each of the following statements, please indicate the extent to which you strongly disagree or strongly agree.

* ***RR1 - My organization respects how the OCR enforces SR compliance.***

Strongly disagree	Disagree	Somewhat disagree	Neither agree or disagree	Somewhat agree	Agree	Strongly agree
☆	☆	☆	☆	☆	☆	☆

* ***RR2 - My organization has a strong, positive relationship with OCR.***

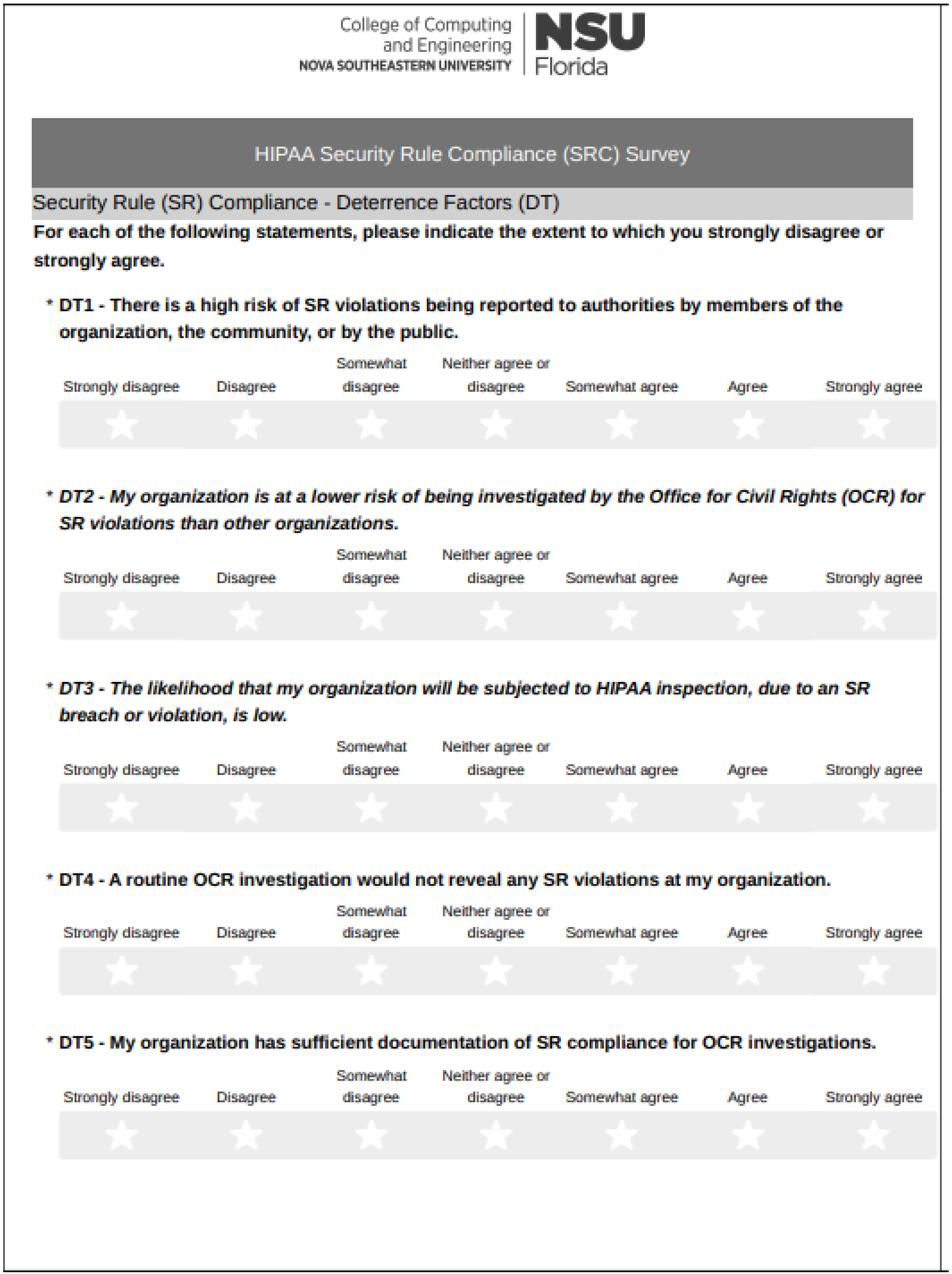
Strongly disagree	Disagree	Somewhat disagree	Neither agree or disagree	Somewhat agree	Agree	Strongly agree
☆	☆	☆	☆	☆	☆	☆

* ***RR3 - My organization respects the OCR judgments, civil money penalties, and resolution agreements relating to SR enforcement.***

Strongly disagree	Disagree	Somewhat disagree	Neither agree or disagree	Somewhat agree	Agree	Strongly agree
☆	☆	☆	☆	☆	☆	☆

8

Appendix H continued:



College of Computing and Engineering
NOVA SOUTHEASTERN UNIVERSITY
NSU Florida

HIPAA Security Rule Compliance (SRC) Survey

Security Rule (SR) Compliance - Deterrence Factors (DT)

For each of the following statements, please indicate the extent to which you strongly disagree or strongly agree.

* **DT1 - There is a high risk of SR violations being reported to authorities by members of the organization, the community, or by the public.**

Strongly disagree	Disagree	Somewhat disagree	Neither agree or disagree	Somewhat agree	Agree	Strongly agree
☆	☆	☆	☆	☆	☆	☆

* ***DT2 - My organization is at a lower risk of being investigated by the Office for Civil Rights (OCR) for SR violations than other organizations.***

Strongly disagree	Disagree	Somewhat disagree	Neither agree or disagree	Somewhat agree	Agree	Strongly agree
☆	☆	☆	☆	☆	☆	☆

* ***DT3 - The likelihood that my organization will be subjected to HIPAA inspection, due to an SR breach or violation, is low.***

Strongly disagree	Disagree	Somewhat disagree	Neither agree or disagree	Somewhat agree	Agree	Strongly agree
☆	☆	☆	☆	☆	☆	☆

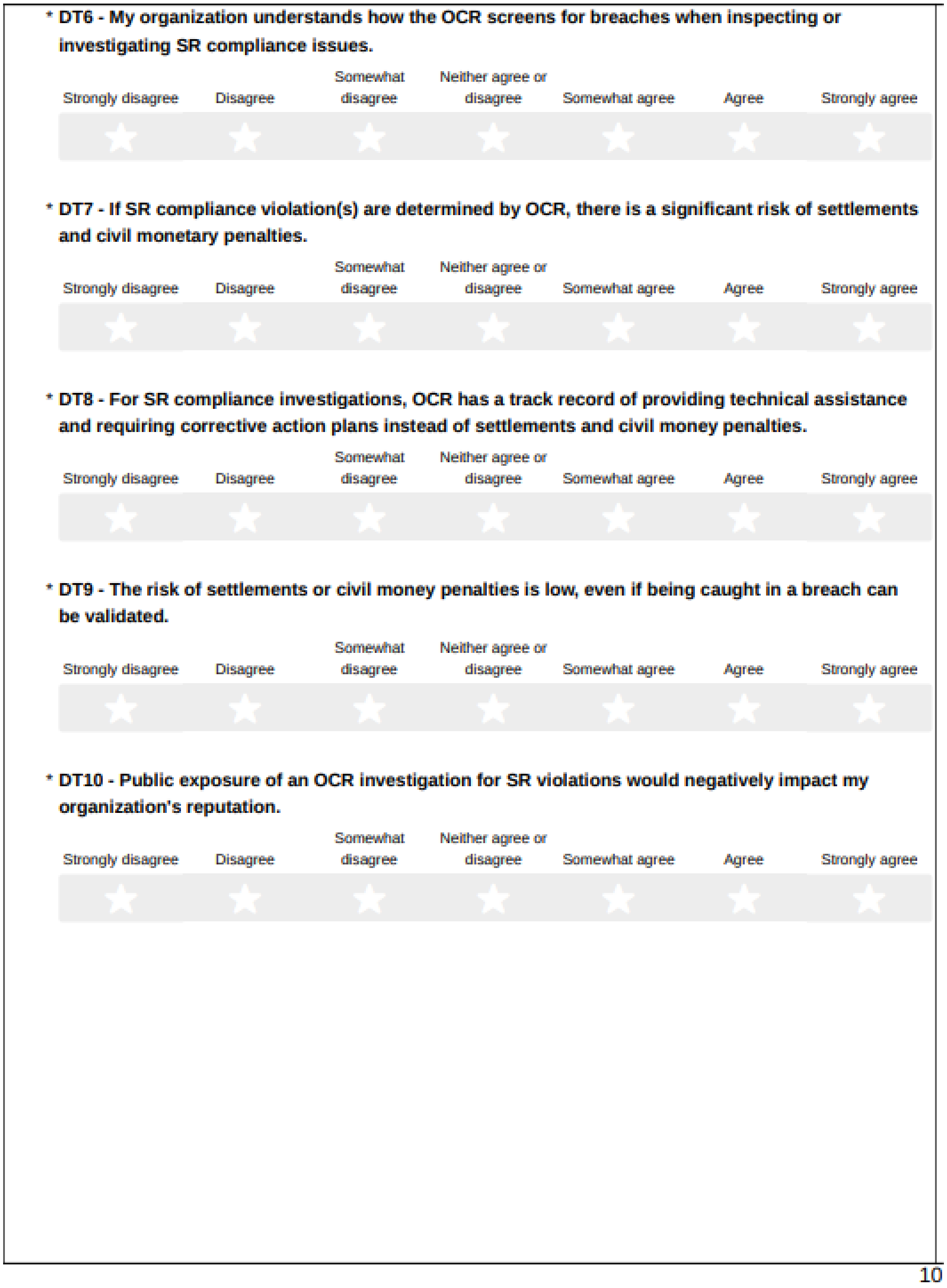
* **DT4 - A routine OCR investigation would not reveal any SR violations at my organization.**

Strongly disagree	Disagree	Somewhat disagree	Neither agree or disagree	Somewhat agree	Agree	Strongly agree
☆	☆	☆	☆	☆	☆	☆

* **DT5 - My organization has sufficient documentation of SR compliance for OCR investigations.**

Strongly disagree	Disagree	Somewhat disagree	Neither agree or disagree	Somewhat agree	Agree	Strongly agree
☆	☆	☆	☆	☆	☆	☆

Appendix H continued:



* DT6 - My organization understands how the OCR screens for breaches when inspecting or investigating SR compliance issues.

Strongly disagree	Disagree	Somewhat disagree	Neither agree or disagree	Somewhat agree	Agree	Strongly agree
☆	☆	☆	☆	☆	☆	☆

* DT7 - If SR compliance violation(s) are determined by OCR, there is a significant risk of settlements and civil monetary penalties.

Strongly disagree	Disagree	Somewhat disagree	Neither agree or disagree	Somewhat agree	Agree	Strongly agree
☆	☆	☆	☆	☆	☆	☆

* DT8 - For SR compliance investigations, OCR has a track record of providing technical assistance and requiring corrective action plans instead of settlements and civil money penalties.

Strongly disagree	Disagree	Somewhat disagree	Neither agree or disagree	Somewhat agree	Agree	Strongly agree
☆	☆	☆	☆	☆	☆	☆

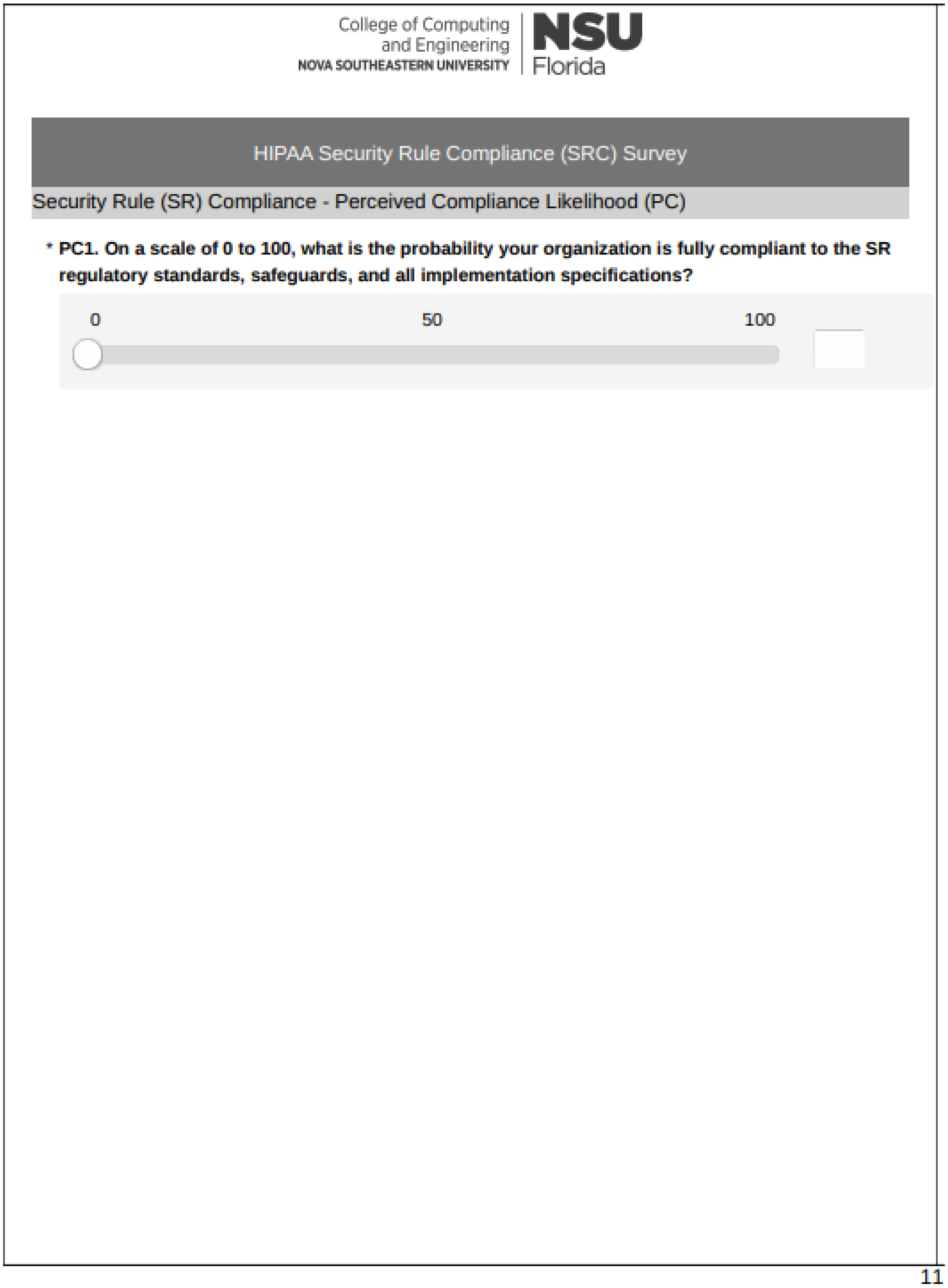
* DT9 - The risk of settlements or civil money penalties is low, even if being caught in a breach can be validated.

Strongly disagree	Disagree	Somewhat disagree	Neither agree or disagree	Somewhat agree	Agree	Strongly agree
☆	☆	☆	☆	☆	☆	☆

* DT10 - Public exposure of an OCR investigation for SR violations would negatively impact my organization's reputation.

Strongly disagree	Disagree	Somewhat disagree	Neither agree or disagree	Somewhat agree	Agree	Strongly agree
☆	☆	☆	☆	☆	☆	☆

Appendix H continued:



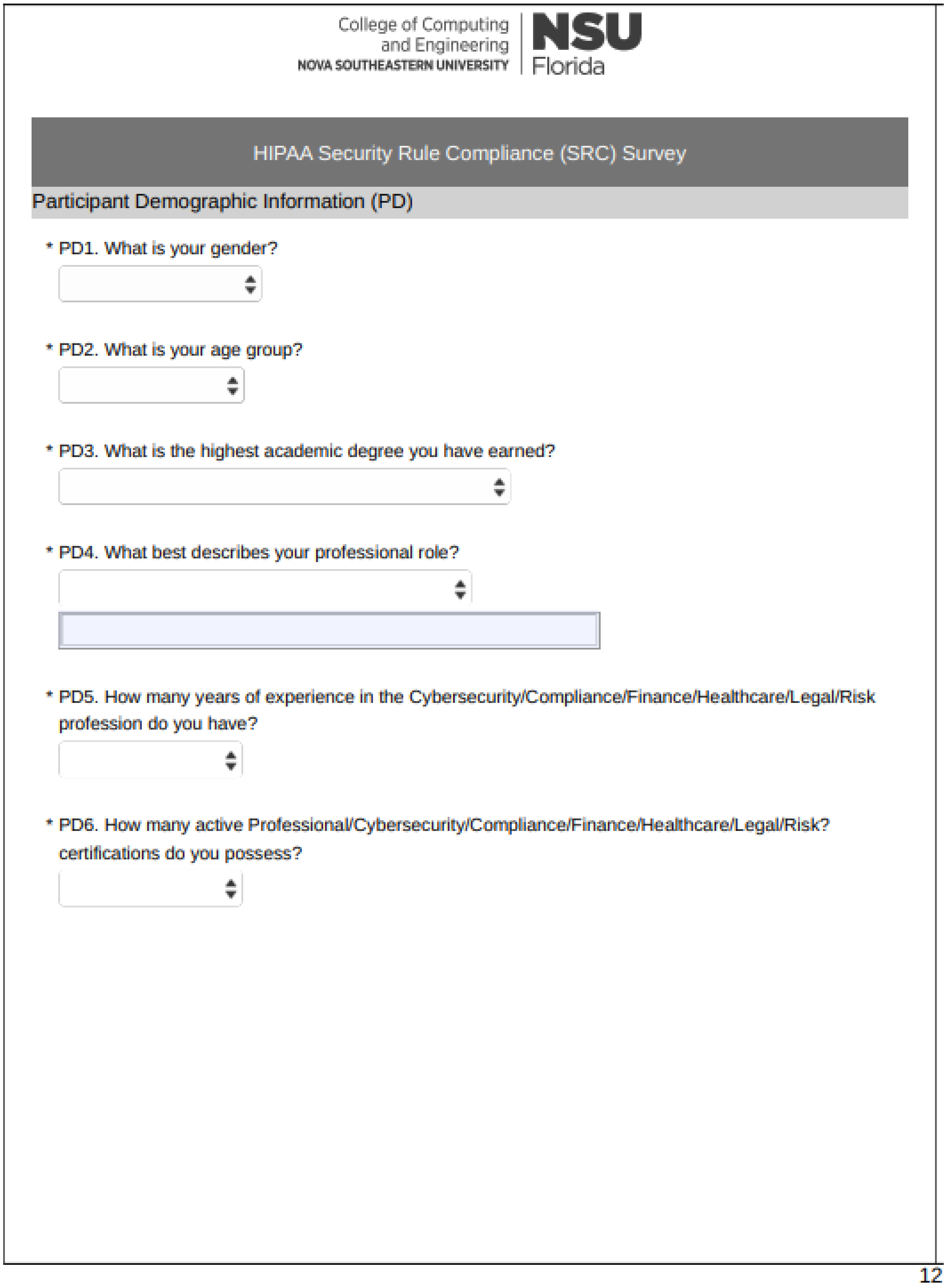
HIPAA Security Rule Compliance (SRC) Survey

Security Rule (SR) Compliance - Perceived Compliance Likelihood (PC)

* PC1. On a scale of 0 to 100, what is the probability your organization is fully compliant to the SR regulatory standards, safeguards, and all implementation specifications?

11

Appendix H continued:



College of Computing
and Engineering
NOVA SOUTHEASTERN UNIVERSITY | NSU Florida

HIPAA Security Rule Compliance (SRC) Survey

Participant Demographic Information (PD)

* PD1. What is your gender?

* PD2. What is your age group?

* PD3. What is the highest academic degree you have earned?

* PD4. What best describes your professional role?

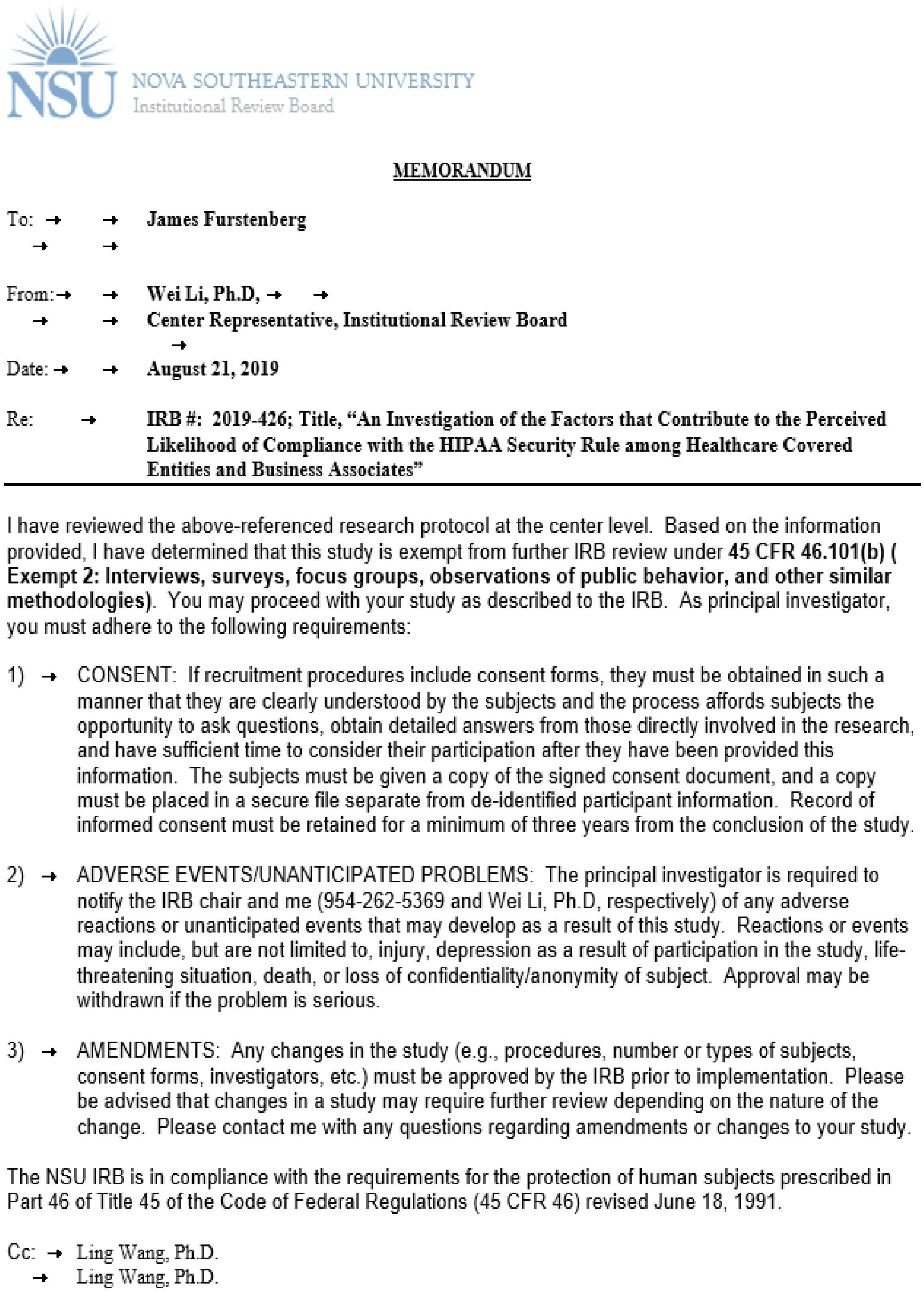
* PD5. How many years of experience in the Cybersecurity/Compliance/Finance/Healthcare/Legal/Risk profession do you have?

* PD6. How many active Professional/Cybersecurity/Compliance/Finance/Healthcare/Legal/Risk? certifications do you possess?

12

Appendix I:

IRB Approval Letter



NSU NOVA SOUTHEASTERN UNIVERSITY
Institutional Review Board

MEMORANDUM

To: → → **James Furstenberg**
→ →

From:→ → **Wei Li, Ph.D, → →**
→ → **Center Representative, Institutional Review Board**
→

Date: → → **August 21, 2019**

Re: → **IRB #: 2019-426; Title, "An Investigation of the Factors that Contribute to the Perceived Likelihood of Compliance with the HIPAA Security Rule among Healthcare Covered Entities and Business Associates"**

I have reviewed the above-referenced research protocol at the center level. Based on the information provided, I have determined that this study is exempt from further IRB review under **45 CFR 46.101(b) (Exempt 2: Interviews, surveys, focus groups, observations of public behavior, and other similar methodologies)**. You may proceed with your study as described to the IRB. As principal investigator, you must adhere to the following requirements:

1) → CONSENT: If recruitment procedures include consent forms, they must be obtained in such a manner that they are clearly understood by the subjects and the process affords subjects the opportunity to ask questions, obtain detailed answers from those directly involved in the research, and have sufficient time to consider their participation after they have been provided this information. The subjects must be given a copy of the signed consent document, and a copy must be placed in a secure file separate from de-identified participant information. Record of informed consent must be retained for a minimum of three years from the conclusion of the study.

2) → ADVERSE EVENTS/UNANTICIPATED PROBLEMS: The principal investigator is required to notify the IRB chair and me (954-262-5369 and Wei Li, Ph.D, respectively) of any adverse reactions or unanticipated events that may develop as a result of this study. Reactions or events may include, but are not limited to, injury, depression as a result of participation in the study, life-threatening situation, death, or loss of confidentiality/anonymity of subject. Approval may be withdrawn if the problem is serious.

3) → AMENDMENTS: Any changes in the study (e.g., procedures, number or types of subjects, consent forms, investigators, etc.) must be approved by the IRB prior to implementation. Please be advised that changes in a study may require further review depending on the nature of the change. Please contact me with any questions regarding amendments or changes to your study.

The NSU IRB is in compliance with the requirements for the protection of human subjects prescribed in Part 46 of Title 45 of the Code of Federal Regulations (45 CFR 46) revised June 18, 1991.

Cc: → Ling Wang, Ph.D.
→ Ling Wang, Ph.D.

Appendix J:

SMEs – Expert Panel SRC Survey Feedback

Page 2: Healthcare Organization Demographics		SME Comments
Q1. What is your organization's primary HIPAA Classification?	Q1. What is your organization's primary HIPAA classification? (Note if hybrid, please choose the option that best represents your HIPAA classification)	
Q2. In what state is your organization headquartered?	Q2. In what state is your organization headquartered?	
Q3. What best represents your organization's business model?	Q3. Please select the organizational business type that best represents your organization.	
Q4. Please select the appropriate industry type that best represents your organization.	Q4. Please select the appropriate industry type that best represents your organization.	
Q5. Please select the appropriate healthcare industry sector that best represents your organization.	Q5. Please select the appropriate healthcare industry sector that best represents your organization.	
Q6. Please indicate the approximate number of full-time employees.	Q6. Please indicate the number (approximate) of full-time employees in your organization.	
Q7. Which of the following professional associations are you most closely affiliated?	Q7. Which of the following professional associations are you affiliated with?	

Page 3: Security Rule Compliance - Motive		
MT1. Complying with the SR costs too much time and money.	MT1. Complying with the SR is too expensive and time-consuming for our organization.	
MT2. Superficial adoption of the SR provides substantial advantages.	MT2. Superficial adoption of the SR provides substantial advantages.	Removed due to ethical considerations - based on attorney advice
MT3. Complying with the SR aligns with our organization's mission(s) and goal(s)	MT3. Complying with the SR aligns with our organization's mission(s) and goal(s)	

Appendix J: continued

MT4. Our organization agrees with the SR regulatory strategy, its policy objectives, and the principles that underpin it.	MT4. My organization agrees with the SR regulatory strategy and its underlying principles of: -- Comprehensiveness. (addresses all aspects of security) -- Scalability- (so it can be effectively implemented by CEs & BAs of all types and sizes), -- Technologically Generic. (not linked to specific technologies).	Altered to clarify SR principles better
MT5. Our organization has effectively put the SR regulatory policy into practice.	MT5. Our organization is highly motivated in implementing the SR requirements/controls.	
MT6.The SR compliance obligations and requirements are acceptable.	MT6. The SR compliance obligations and requirements have negatively impacted opportunities for business growth (expansion).	
MT7. Compliance with the SR is beneficial despite the specific safeguards and obligations.	MT7. Compliance with the SR is beneficial in safeguarding and protecting ePHI.	
MT8. Our organization's adoption of SR compliance is influenced by industry groups, regulators, customers, investors, trading partners communities, non-governmental organizations, or any other stakeholders.	MT8 - Adoption of SR compliance practices are strongly influenced by industry groups, customers, investors, trading partner communities, non-governmental organizations, and/or other stakeholders.	

Page 4: Security Rule Compliance - Organizational Characteristic & Capacities	
CC1. SR compliance is relevant to our organization's business model.	CC1. Complying with the SR regulatory obligations is an essential part of my organization's business model?
CC2. Our organization is fully aware of the SR standards and their obligations.	CC2. Our organization is fully aware of the SR standards and implementation specifications.
CC3. Our organization knows the SR standards and implementation specifications that govern compliance requirements).	CC3. There are appropriate levels of management support for implementing and monitoring SR compliance in my organization.
CC4. The SR is too complex to comply with or to implement fully).	CC4. The SR is too complex to comply with or to implement fully.

Appendix J: continued

CC5. Our organization provides adequate funding for SR compliance and implementation).	CC5. Our organization provides adequate funding for SR compliance and implementation.
CC6. Our organization has the necessary level of technical expertise to comply with, implement, and monitor SR compliance).	CC6. Our organization has the professional/technical expertise to comply with, implement, and monitor SR compliance.
CC7. Our organization devotes an appropriate amount of time to implementing and monitoring SR compliance).	CC7. Our organization devotes an appropriate amount of organizational focus toward implementing and monitoring SR compliance.
CC8. There are appropriate level management systems and management support to implement and monitor SR compliance).	CC8. There are appropriate levels of hardware, software, and information management systems for implementing and monitoring SR compliance activities in my organization.

Page 5: Security Rule Compliance - Regulator Respect	
RR1. Our organization respects how the Office for Civil Rights (OCR) educates and supports organizations regarding SR compliance).	RR1. My organization values the support (education, training, and resources) the Office for Civil Rights (OCR) provides toward SR compliance.
RR2. Our organization respects how the OCR enforces SR compliance).	RR2. Our organization respects how the regulator (Office for Civil Rights) goes about enforcing SR compliance.
RR3. Our organization has a strong, positive relationship with OCR).	RR3. Our organization has a strong, positive relationship with OCR.
RR4. Our organization respects the OCR judgments, civil money penalties, and resolution agreements relating to SR enforcement).	RR4. Our organization respects the Office for Civil Rights' judgments, civil monetary fines, and resolution agreements relating to SR enforcement.

Page 6: Security Rule Compliance - Deterrence Factors	
DT1. There is a high risk of SR violations being reported to the authorities either by members of our organization, our patients/customers, or third parties with whom we work).	DT1. There is a high risk of SR violations being reported to the authorities by members of the organization, the community, or by the public.

Appendix J: continued

DT2. Our organization’s compliance with the SR is due to fear of violations, complaints, or reports).	DT2. Our organization’s compliance with the SR is due to fear of violations, complaints, or reports.	
DT3. Our organization is at a lower risk of being investigated by the OCR for SR violations than other organizations).	DT3. Our organization is at a lower risk of being investigated by the OCR for SR violations than other organizations.	
DT4. The likelihood that our organization will be subjected to an OCR investigation, due to a breach or other violation is very low).	DT4. The likelihood that our organization will be subjected to HIPAA inspection due to an SR breach or violation is low.	
DT5. An OCR audit would not reveal any SR violations at our organization).	DT5. A routine OCR investigation would not reveal any SR violations at my organization.	
DT6. The integrity of our SR compliance documentation is such that it would be difficult for OCR investigators to detect a lack of compliance).	DT6. My organization has sufficient documentation of SR compliance for OCR investigations.	
DT7. The risk of an SR violation being detected is low in our organization).	DT7. The risk of an SR violation being detected is low in our organization.	Removed redundant with DT5
DT8 - Feedback- (The OCR is selective in identifying and prioritizing organizations for enforcement activity (e.g., compliance reviews, audits, or investigations).	DT8. The OCR enforcement priority (e.g., compliance reviews or investigations) is largely based on the number of ePHI records involved.	
DT9. Our organization falls outside of the priority targets for SR compliance enforcement).	DT9. Our organization falls outside of the priority targets for SR compliance enforcement	Construct measured in DT5-8
DT10. Our organization understands how OCR screens for breaches when investigating SR compliance issues).	DT10. My organization understands how the Office for Civil Rights screens for breaches when inspecting or investigating SR compliance issues.	
DT11. If an SR compliance violation is determined by OCR, there is a significant risk of sanctioning).	DT11. If SR compliance violation(s) are determined by OCR, there is a significant risk of settlements and civil monetary penalties.	
DT12. OCR has a track record of dismissing more cases than it pursues through a resolution agreement).	DT12. For SR compliance investigations, OCR has a track record of providing technical assistance and requiring corrective action plans instead of settlements and civil money penalties.	

Appendix J: continued

DT13. The risk of a monetary sanction is low, even if SR violations which can be proven).	DT13. The risk of settlements or civil money penalties is low, even if being caught in a breach can be proved.	
DT14. Sanctions for violations of SR compliance will be imposed quickly by OCR).	DT14. Sanctions for violations of SR compliance will be imposed quickly by OCR	Removed timeliness is too subjective
DT15. SR violations and civil money penalties would negatively impact our organization).	DT15. Public exposure of an OCR investigation for SR violations would negatively impact our organization's reputation.	

Page 7: Security Rule Compliance - Perceived Compliance Likelihood	
PC1. Our organization is fully compliant with SR regulatory standards and implementation specifications.	PC1. Our organization is fully compliant with SR regulatory standards and implementation specifications

Appendix K

SRC Pilot to Final Survey IVs Question Numbering Changes

Construct	Pilot Q #	Changes	Final Survey Q#
Motives (MT)			
	MT1	Removed	
	MT2	MT2	MT1
	MT3	MT3	MT2
	MT4	MT4	MT3
Characteristics & Capacities (CC)			
	CC1 -CC8		CC1-CC8
		Remains the same	
Regulator Respect (RR)			
	RR1	Removed	
	RR2	RR2	RR1
	RR3	RR3	RR2
	RR4	RR4	RR3
Deterrence Factors (DT)			
	DT1	DT1	DT1
	DT2	Removed	
	DT3	DT3	DT2
	DT4	DT4	DT3
	DT5	DT5	DT4
	DT6	DT6	DT5
	DT7	Removed	
	DT8	DT8	DT6
	DT9	DT9	DT7
	DT10	DT10	DT8
	DT11	DT11	DT9
	DT12	DT12	DT10

Appendix L

Frequency Tables for All Survey Questions

Do you agree to informed consent?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	114	100.0	100.0	100.0

1. What is your organization's primary HIPAA classification?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Covered Entity	75	65.8	65.8	65.8
	Business Associate	39	34.2	34.2	100.0
	Total	114	100.0	100.0	

2. In what state is your organization headquartered?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Alabama	1	0.9	0.9	0.9
	Arizona	2	1.8	1.8	2.6
	Arkansas	1	0.9	0.9	3.5
	California	7	6.1	6.1	9.6
	Colorado	1	0.9	0.9	10.5
	Connecticut	2	1.8	1.8	12.3
	Delaware	1	0.9	0.9	13.2
	Florida	6	5.3	5.3	18.4
	Georgia	1	0.9	0.9	19.3
	Hawaii	1	0.9	0.9	20.2
	Illinois	5	4.4	4.4	24.6
	Indiana	3	2.6	2.6	27.2
	Kentucky	1	0.9	0.9	28.1
	Maryland	1	0.9	0.9	28.9
	Michigan	35	30.7	30.7	59.6
	Minnesota	2	1.8	1.8	61.4
	Mississippi	1	0.9	0.9	62.3
	New Jersey	3	2.6	2.6	64.9
	New York	5	4.4	4.4	69.3

	North Carolina	2	1.8	1.8	71.1
	North Dakota	1	0.9	0.9	71.9
	Ohio	3	2.6	2.6	74.6
	Oregon	2	1.8	1.8	76.3
	Pennsylvania	3	2.6	2.6	78.9
	South Dakota	1	0.9	0.9	79.8
	Tennessee	7	6.1	6.1	86.0
	Texas	11	9.6	9.6	95.6
	Virginia	3	2.6	2.6	98.2
	Washington	2	1.8	1.8	100.0
	Total	114	100.0	100.0	

3. What best represents your organization's business model?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Non-Profit	57	50.0	50.0	50.0
	Profit	57	50.0	50.0	100.0
	Total	114	100.0	100.0	

4. Which industry type best represents your organization?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Business services	5	4.4	4.4	4.4
	Consulting	9	7.9	7.9	12.3
	Education	10	8.8	8.8	21.1
	Other	2	1.8	1.8	22.8
	Government	2	1.8	1.8	24.6
	Health Care	68	59.6	59.6	84.2
	Hospitality	1	0.9	0.9	85.1
	Insurance	2	1.8	1.8	86.8
	Manufacturing	2	1.8	1.8	88.6
	Pharmaceutical	1	0.9	0.9	89.5
	Retail	1	0.9	0.9	90.4
	Technology	11	9.6	9.6	100.0
	Total	114	100.0	100.0	

5. Which healthcare industry sector best represents your organization?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Academic Medical Center	15	13.2	13.2	13.2
	Ambulatory Care	3	2.6	2.6	15.8
	Behavioral Care	4	3.5	3.5	19.3
	Billing Services/Claims Processing	4	3.5	3.5	22.8
	Business Process Outsourcing	2	1.8	1.8	24.6
	Clinic (for-profit)	4	3.5	3.5	28.1
	Clinic (nonprofit)	2	1.8	1.8	29.8
	Clinical Laboratory Services	1	0.9	0.9	30.7
	Contract Management	1	0.9	0.9	31.6
	Cyber Risk Management	11	9.6	9.6	41.2
	Dental Services	3	2.6	2.6	43.9
	Federally Qualified Health Center	1	0.9	0.9	44.7
	Government Agency	2	1.8	1.8	46.5
	Health Information Exchange	3	2.6	2.6	49.1
	Health Information Technology	9	7.9	7.9	57.0
	Health Insurance	3	2.6	2.6	59.6
	Health System	21	18.4	18.4	78.1
	Hospital Owner Management Company	3	2.6	2.6	80.7
	Integrated Health System	4	3.5	3.5	84.2
	Medical Equipment or Devices	4	3.5	3.5	87.7
	Occupational (or Employee or Corporate) Wellness Program	1	0.9	0.9	88.6
	Optical Retail	2	1.8	1.8	90.4
	Pediatric Care/Services	1	0.9	0.9	91.2
	Pharmaceutical Company	1	0.9	0.9	92.1

	Radiology/Picture Archiving and Communication System (PACS)	1	0.9	0.9	93.0
	University (nonprofit)	4	3.5	3.5	96.5
	University (private)	1	0.9	0.9	97.4
	Other	3	2.6	2.6	100.0
	Total	114	100.0	100.0	

6. Approximately how many full-time employees are there in your organization?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1-9	10	8.8	8.8	8.8
	10-49	7	6.1	6.1	14.9
	50-99	11	9.6	9.6	24.6
	100 - 499	17	14.9	14.9	39.5
	500 -999	4	3.5	3.5	43.0
	1000-1999	6	5.3	5.3	48.2
	2000-3999	9	7.9	7.9	56.1
	4000 +	49	43.0	43.0	99.1
	Decline to respond	1	0.9	0.9	100.0
	Total	114	100.0	100.0	

7.1 Are you a member of the Ambulatory Surgery Center Assoc?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	113	99.1	99.1	99.1
	Yes	1	0.9	0.9	100.0
	Total	114	100.0	100.0	

7.2 Are you a member of the American College of Healthcare Executives - (ACHE)?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	103	90.4	90.4	90.4
	Yes	11	9.6	9.6	100.0
	Total	114	100.0	100.0	

7.3 Are you a member of the American Health Care Association?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	107	93.9	93.9	93.9
	Yes	7	6.1	6.1	100.0
	Total	114	100.0	100.0	

7.4 Are you a member of the American Health Information Management Association -(AHIMA)?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	87	76.3	76.3	76.3
	Yes	27	23.7	23.7	100.0
	Total	114	100.0	100.0	

7.5 Are you a member of the American Health Lawyers Association - (AHLA)?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	104	91.2	91.2	91.2
	Yes	10	8.8	8.8	100.0
	Total	114	100.0	100.0	

7.6 Are you a member of the American Hospital Association?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	95	83.3	83.3	83.3
	Yes	19	16.7	16.7	100.0
	Total	114	100.0	100.0	

7.7 Are you a member of the American Medical Association?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	92	80.7	80.7	80.7
	Yes	22	19.3	19.3	100.0
	Total	114	100.0	100.0	

7.8 Are you a member of the American Medical Informatics Association?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	105	92.1	92.1	92.1
	Yes	9	7.9	7.9	100.0
	Total	114	100.0	100.0	

7.9 Are you a member of the American Osteopathic Association?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	112	98.2	98.2	98.2
	Yes	2	1.8	1.8	100.0
	Total	114	100.0	100.0	

7.10 Are you a member of the Association for Executives in Healthcare Information Security (AEHIS)?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	80	70.2	70.2	70.2
	Yes	34	29.8	29.8	100.0
	Total	114	100.0	100.0	

7.11 Are you a member of the College of Healthcare Information Management Executives - (CHIME)?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	74	64.9	64.9	64.9
	Yes	40	35.1	35.1	100.0
	Total	114	100.0	100.0	

7.12 Are you a member of the Health Care Compliance Association - (HCCA)?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	84	73.7	73.7	73.7
	Yes	30	26.3	26.3	100.0
	Total	114	100.0	100.0	

7.13 Are you a member of the Healthcare Financial Management Association - (HFMA)?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	104	91.2	91.2	91.2
	Yes	10	8.8	8.8	100.0
	Total	114	100.0	100.0	

7.14 Are you a member of the International Association of Privacy Professionals -(IAPP)?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	88	77.2	77.2	77.2
	Yes	26	22.8	22.8	100.0
	Total	114	100.0	100.0	

7.15 Are you a member of the Society of Information Risk Analysts - (SIRA)?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	112	98.2	98.2	98.2
	Yes	2	1.8	1.8	100.0
	Total	114	100.0	100.0	

7.16 Are you a member of The Joint Commission?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	108	94.7	94.7	94.7
	Yes	6	5.3	5.3	100.0
	Total	114	100.0	100.0	

7.17 Do you know if you are a member of an association?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	85	74.6	74.6	74.6
	Yes	29	25.4	25.4	100.0
	Total	114	100.0	100.0	

7.18 Do you decline to report your association affiliations?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	108	94.7	94.7	94.7
	Yes	6	5.3	5.3	100.0
	Total	114	100.0	100.0	

7.19 Are you a member of some other associations?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ACFE	1	0.9	0.9	0.9
	American Dental Association	1	0.9	0.9	1.8
	American Optometric Association	1	0.9	0.9	2.6
	Association of American Medical Colleges	1	0.9	0.9	3.5
	CARF	1	0.9	0.9	4.4
	Commission on Dental Accreditation through the American Dental Association, American Dental Hygiene Association, Michigan Dental Hygiene Association, Michigan Dental Association	1	0.9	0.9	5.3
	H-ISAC, Infragard	1	0.9	0.9	6.1
	Health Information and Management Systems Society (HIMSS)& American College of Clinical Engineering	1	0.9	0.9	7.0
	HIMSS	2	1.8	1.8	8.8
	HIMSS and others	1	0.9	0.9	9.6
	HIMSS, ISACA, ISC(2)	1	0.9	0.9	10.5
	ISACA	1	0.9	0.9	11.4
	ISACA, (ISC)2	1	0.9	0.9	12.3
	ISACA, ISC2	1	0.9	0.9	13.2
	ISC2	1	0.9	0.9	14.0

Medical Group Management Association MGMA	1	0.9	0.9	14.9
Michigan Association of CMH Boards, CARF, etc.	1	0.9	0.9	15.8
National Assoc. of Chain Drug Stores	1	0.9	0.9	16.7
None	93	81.6	81.6	98.2
Our Health Department is a member of quite a few organizations, but I am not aware off them offhand.	1	0.9	0.9	99.1
x12.org & WEDI.org	1	0.9	0.9	100.0
Total	114	100.0	100.0	

Appendix M

Motive Descriptive Statistics - Frequency

MT1. Complying with the SR aligns with my organization's mission(s) and goal(s).

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Somewhat Disagree	2	1.8	1.8	1.8
	Neither Agree or Disagree	2	1.8	1.8	3.5
	Somewhat Agree	11	9.6	9.6	13.2
	Agree	52	45.6	45.6	58.8
	Strongly Agree	47	41.2	41.2	100.0
	Total	114	100.0	100.0	

MT2. My organization agrees with the SR regulatory strategy and its underlying principles of: Comprehensiveness, Scalability, and Technologically Generic.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Disagree	1	0.9	0.9	0.9
	Somewhat Disagree	2	1.8	1.8	2.6
	Neither Agree or Disagree	12	10.5	10.5	13.2
	Somewhat Agree	29	25.4	25.4	38.6
	Agree	38	33.3	33.3	71.9
	Strongly Agree	32	28.1	28.1	100.0
	Total	114	100.0	100.0	

MT3. My organization is highly motivated in implementing the SR requirements/controls.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Somewhat Disagree	4	3.5	3.5	3.5
	Neither Agree or Disagree	6	5.3	5.3	8.8
	Somewhat Agree	23	20.2	20.2	28.9
	Agree	48	42.1	42.1	71.1
	Strongly Agree	33	28.9	28.9	100.0
	Total	114	100.0	100.0	

Appendix N

Characteristics & Capacities Descriptive Statistics - Frequency

CC1. Complying with the SR regulatory obligations is an essential part of my organization's business model?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Disagree	3	2.6	2.6	2.6
	Somewhat Disagree	3	2.6	2.6	5.3
	Neither Agree or Disagree	9	7.9	7.9	13.2
	Somewhat Agree	16	14.0	14.0	27.2
	Agree	53	46.5	46.5	73.7
	Strongly Agree	30	26.3	26.3	100.0
	Total	114	100.0	100.0	

CC2. My organization is fully aware of the SR standards and implementation specifications.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Somewhat Disagree	3	2.6	2.6	2.6
	Neither Agree or Disagree	10	8.8	8.8	11.4
	Somewhat Agree	21	18.4	18.4	29.8
	Agree	45	39.5	39.5	69.3
	Strongly Agree	35	30.7	30.7	100.0
	Total	114	100.0	100.0	

CC3. There are appropriate levels of management support for implementing and monitoring SR compliance in my organization.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Disagree	4	3.5	3.5	3.5
	Somewhat Disagree	8	7.0	7.0	10.5
	Neither Agree or Disagree	7	6.1	6.1	16.7
	Somewhat Agree	31	27.2	27.2	43.9
	Agree	39	34.2	34.2	78.1
	Strongly Agree	25	21.9	21.9	100.0
	Total	114	100.0	100.0	

CC4. The SR is too complex to comply with or to implement fully.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	8	7.0	7.0	7.0
	Disagree	14	12.3	12.3	19.3
	Somewhat Disagree	19	16.7	16.7	36.0
	Neither Agree or Disagree	28	24.6	24.6	60.5
	Somewhat Agree	29	25.4	25.4	86.0
	Agree	13	11.4	11.4	97.4
	Strongly Agree	3	2.6	2.6	100.0
	Total	114	100.0	100.0	

CC5. My organization provides adequate funding for SR compliance and implementation.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	4	3.5	3.5	3.5
	Disagree	5	4.4	4.4	7.9
	Somewhat Disagree	20	17.5	17.5	25.4
	Neither Agree or Disagree	20	17.5	17.5	43.0
	Somewhat Agree	29	25.4	25.4	68.4
	Agree	24	21.1	21.1	89.5
	Strongly Agree	12	10.5	10.5	100.0
	Total	114	100.0	100.0	

CC6. My organization has the professional/technical expertise to comply with, implement, and monitor SR compliance.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	2	1.8	1.8	1.8
	Disagree	3	2.6	2.6	4.4
	Somewhat Disagree	20	17.5	17.5	21.9
	Neither Agree or Disagree	13	11.4	11.4	33.3
	Somewhat Agree	31	27.2	27.2	60.5
	Agree	27	23.7	23.7	84.2
	Strongly Agree	18	15.8	15.8	100.0

	Total	114	100.0	100.0	

CC7. My organization devotes an appropriate amount of organizational focus toward implementing and monitoring SR compliance.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	1	0.9	0.9	0.9
	Disagree	3	2.6	2.6	3.5
	Somewhat Disagree	18	15.8	15.8	19.3
	Neither Agree or Disagree	14	12.3	12.3	31.6
	Somewhat Agree	41	36.0	36.0	67.5
	Agree	27	23.7	23.7	91.2
	Strongly Agree	10	8.8	8.8	100.0
	Total	114	100.0	100.0	

CC8. There are appropriate levels of hardware, software, and information management systems for implementing and monitoring SR compliance activities in my organization.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	3	2.6	2.6	2.6
	Disagree	5	4.4	4.4	7.0
	Somewhat Disagree	20	17.5	17.5	24.6
	Neither Agree or Disagree	12	10.5	10.5	35.1
	Somewhat Agree	35	30.7	30.7	65.8
	Agree	28	24.6	24.6	90.4
	Strongly Agree	11	9.6	9.6	100.0
	Total	114	100.0	100.0	

Appendix O

Regulator Respect Descriptive Statistics - Frequency

RR1. My organization respects how the OCR enforces SR compliance.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Disagree	2	1.8	1.8	1.8
	Somewhat Disagree	7	6.1	6.1	7.9
	Neither Agree or Disagree	42	36.8	36.8	44.7
	Somewhat Agree	22	19.3	19.3	64.0
	Agree	30	26.3	26.3	90.4
	Strongly Agree	11	9.6	9.6	100.0
	Total	114	100.0	100.0	

RR2. My organization has a strong, positive relationship with OCR.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	1	0.9	0.9	0.9
	Disagree	1	0.9	0.9	1.8
	Somewhat Disagree	5	4.4	4.4	6.1
	Neither Agree or Disagree	59	51.8	51.8	57.9
	Somewhat Agree	13	11.4	11.4	69.3
	Agree	23	20.2	20.2	89.5
	Strongly Agree	12	10.5	10.5	100.0
	Total	114	100.0	100.0	

RR3. My organization respects the OCR judgments, civil money penalties, and resolution agreements relating to SR enforcement.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Somewhat Disagree	8	7.0	7.0	7.0
	Neither Agree or Disagree	45	39.5	39.5	46.5
	Somewhat Agree	17	14.9	14.9	61.4
	Agree	30	26.3	26.3	87.7
	Strongly Agree	14	12.3	12.3	100.0
	Total	114	100.0	100.0	

Appendix P:

Deterrence Factors Descriptive Statistics - Frequency

DT1. There is a high risk of SR violations being reported to authorities by members of the organization, the community, or by the public.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	3	2.6	2.6	2.6
	Disagree	10	8.8	8.8	11.4
	Somewhat Disagree	12	10.5	10.5	21.9
	Neither Agree or Disagree	24	21.1	21.1	43.0
	Somewhat Agree	24	21.1	21.1	64.0
	Agree	26	22.8	22.8	86.8
	Strongly Agree	15	13.2	13.2	100.0
	Total	114	100.0	100.0	

DT2. My organization is at a lower risk of being investigated by the Office for Civil Rights (OCR) for SR violations than other organizations.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	11	9.6	9.6	9.6
	Disagree	9	7.9	7.9	17.5
	Somewhat Disagree	9	7.9	7.9	25.4
	Neither Agree or Disagree	40	35.1	35.1	60.5
	Somewhat Agree	19	16.7	16.7	77.2
	Agree	18	15.8	15.8	93.0
	Strongly Agree	8	7.0	7.0	100.0
	Total	114	100.0	100.0	

DT3. The likelihood that my organization will be subjected to HIPAA inspection due to an SR breach or violation is low.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	8	7.0	7.0	7.0
	Disagree	9	7.9	7.9	14.9
	Somewhat Disagree	17	14.9	14.9	29.8
	Neither Agree or Disagree	35	30.7	30.7	60.5
	Somewhat Agree	26	22.8	22.8	83.3
	Agree	14	12.3	12.3	95.6

	Strongly Agree	5	4.4	4.4	100.0
	Total	114	100.0	100.0	

***DT4. A routine OCR investigation would not reveal any SR violations at my organization*.**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	4	3.5	3.5	3.5
	Disagree	15	13.2	13.2	16.7
	Somewhat Disagree	29	25.4	25.4	42.1
	Neither Agree or Disagree	30	26.3	26.3	68.4
	Somewhat Agree	15	13.2	13.2	81.6
	Agree	16	14.0	14.0	95.6
	Strongly Agree	5	4.4	4.4	100.0
	Total	114	100.0	100.0	

DT5.My organization has sufficient documentation of SR compliance for OCR investigations.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	3	2.6	2.6	2.6
	Disagree	7	6.1	6.1	8.8
	Somewhat Disagree	18	15.8	15.8	24.6
	Neither Agree or Disagree	19	16.7	16.7	41.2
	Somewhat Agree	22	19.3	19.3	60.5
	Agree	37	32.5	32.5	93.0
	Strongly Agree	8	7.0	7.0	100.0
	Total	114	100.0	100.0	

***DT6. My organization understands how the OCR screens for breaches when inspecting or investigating SR compliance issues*.**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	1	0.9	0.9	0.9
	Disagree	9	7.9	7.9	8.8
	Somewhat Disagree	19	16.7	16.7	25.4
	Neither Agree or Disagree	25	21.9	21.9	47.4

	Somewhat Agree	27	23.7	23.7	71.1
	Agree	19	16.7	16.7	87.7
	Strongly Agree	14	12.3	12.3	100.0
	Total	114	100.0	100.0	

DT7. If SR compliance violation(s) are determined by OCR, there is a significant risk of settlements and civil monetary penalties.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	2	1.8	1.8	1.8
	Disagree	2	1.8	1.8	3.5
	Somewhat Disagree	7	6.1	6.1	9.6
	Neither Agree or Disagree	14	12.3	12.3	21.9
	Somewhat Agree	22	19.3	19.3	41.2
	Agree	49	43.0	43.0	84.2
	Strongly Agree	18	15.8	15.8	100.0
	Total	114	100.0	100.0	

DT8. For SR compliance investigations, OCR has a track record of providing technical assistance and requiring corrective action plans instead of settlements and civil money penalties.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	1	0.9	0.9	0.9
	Disagree	5	4.4	4.4	5.3
	Somewhat Disagree	15	13.2	13.2	18.4
	Neither Agree or Disagree	55	48.2	48.2	66.7
	Somewhat Agree	20	17.5	17.5	84.2
	Agree	15	13.2	13.2	97.4
	Strongly Agree	3	2.6	2.6	100.0
	Total	114	100.0	100.0	

DT9. The risk of settlements or civil money penalties is low, even if being caught in a breach can be validated.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	15	13.2	13.2	13.2
	Disagree	30	26.3	26.3	39.5
	Somewhat Disagree	20	17.5	17.5	57.0

	Neither Agree or Disagree	29	25.4	25.4	82.5
	Somewhat Agree	8	7.0	7.0	89.5
	Agree	9	7.9	7.9	97.4
	Strongly Agree	3	2.6	2.6	100.0
	Total	114	100.0	100.0	

DT10. Public exposure of an OCR investigation for SR violations would negatively impact my organization's reputation.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Disagree	1	0.9	0.9	0.9
	Somewhat Disagree	1	0.9	0.9	1.8
	Neither Agree or Disagree	6	5.3	5.3	7.0
	Somewhat Agree	8	7.0	7.0	14.0
	Agree	34	29.8	29.8	43.9
	Strongly Agree	64	56.1	56.1	100.0
	Total	114	100.0	100.0	

Appendix Q:

Population Demographics Descriptive Statistics - Frequency

PD1. What is your gender?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Female	30	26.3	26.3	26.3
	Male	74	64.9	64.9	91.2
	Prefer not to respond	10	8.8	8.8	100.0
	Total	114	100.0	100.0	

PD2.What is your age group?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	20 to 29 years	4	3.5	3.5	3.5
	30 to 39 years	9	7.9	7.9	11.4
	40 to 49 years	30	26.3	26.3	37.7
	50 to 59 years	43	37.7	37.7	75.4
	Over 60 years	18	15.8	15.8	91.2
	Decline to respond	10	8.8	8.8	100.0
	Total	114	100.0	100.0	

PD3. What is the highest academic degree you have earned?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	High school diploma or equivalent (e.g. GED)	1	0.9	0.9	0.9
	Some college, no degree	6	5.3	5.3	6.1
	Associates degree (2-year college)	3	2.6	2.6	8.8
	Bachelor’s degree (4-year college)	48	42.1	42.1	50.9
	Graduate degree (Masters, Professional, Doctorate)	53	46.5	46.5	97.4
	Decline to respond	3	2.6	2.6	100.0
	Total	114	100.0	100.0	

PD4. What best describes your professional role?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Attorney	3	2.6	2.6	2.6
	Billing and Coding	2	1.8	1.8	4.4
	Compliance (General)	9	7.9	7.9	12.3
	Compliance (HIPAA)	13	11.4	11.4	23.7
	Cyber Security Professional (analyst, engineer)	15	13.2	13.2	36.8
	Health System Transactions	1	0.9	0.9	37.7
	Hospitals/Health Systems	6	5.3	5.3	43.0
	Information Security Analyst	6	5.3	5.3	48.2
	Information Security Manager	13	11.4	11.4	59.6
	Practice Management/Physician Practice	3	2.6	2.6	62.3
	Risk Management	1	0.9	0.9	63.2
	Security Consultant	2	1.8	1.8	64.9
	Sr Executive (CISO, CEO, COO, etc.)	30	26.3	26.3	91.2
	Decline to respond	9	7.9	7.9	99.1
	Other (please specify)	1	0.9	0.9	100.0
	Total	114	100.0	100.0	

PD5. How many years of experience in the Cybersecurity/Compliance/Finance/Healthcare/Legal/Risk profession do you have?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	less than 2 years	1	0.9	0.9	0.9
	1 - 5 years	15	13.2	13.2	14.0
	6 - 10 years	19	16.7	16.7	30.7
	11 - 15 years	28	24.6	24.6	55.3
	16 - 20 years	19	16.7	16.7	71.9
	20 years or more	28	24.6	24.6	96.5
	Decline to respond	4	3.5	3.5	100.0

	Total	114	100.0	100.0	

PD6. How many active Professional/Cybersecurity/Compliance/Finance/Healthcare/Legal/Risk certifications do you possess?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0	18	15.8	15.8	15.8
	1	24	21.1	21.1	36.8
	2	29	25.4	25.4	62.3
	3	18	15.8	15.8	78.1
	4	7	6.1	6.1	84.2
	5 or more	14	12.3	12.3	96.5
	Decline to respond	4	3.5	3.5	100.0
	Total	114	100.0	100.0	

Appendix R:

Multiple Linear Regression - Evaluation of Assumptions for all IVs

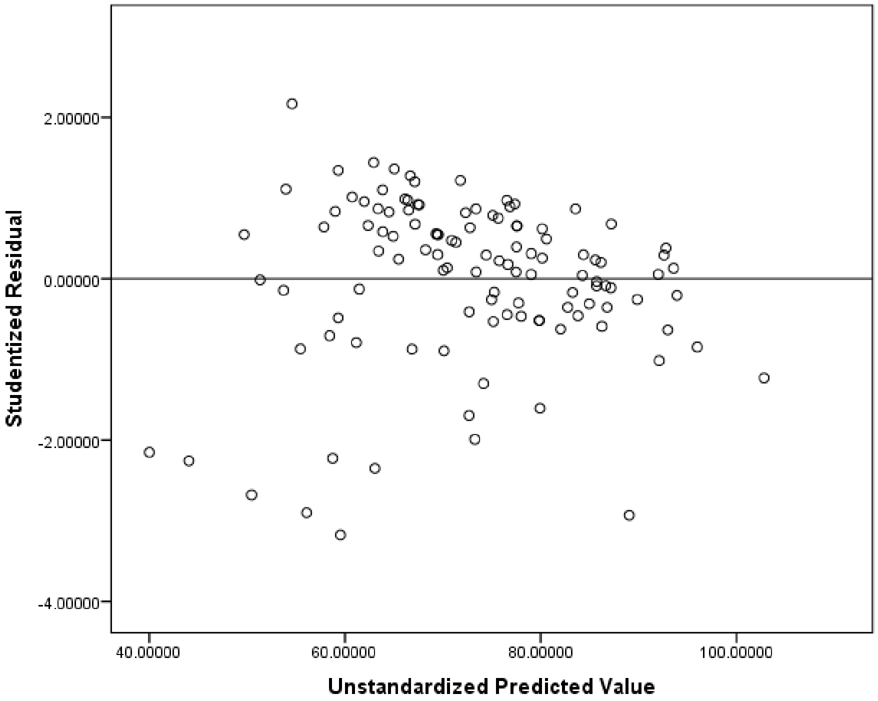


Figure R1. Evaluating the Linearity assumption that the IVs (MT, CC, RR & DT) collectively have a linear relationship with the DV (PC1)

Appendix R: continued

MLR- MT Evaluation of Assumptions for Multiple Linear Regression

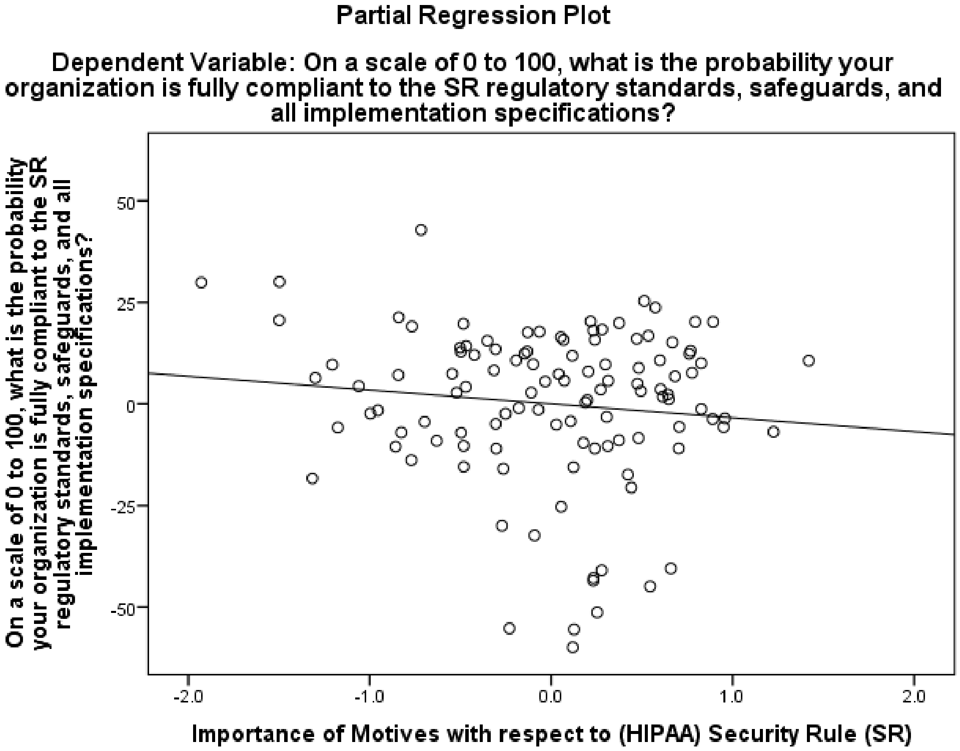


Figure R2. Motives: Evaluating the Linearity assumption that the IV of MT individually have a linear relationship with the DV (PC1).

Appendix R: continued

MLR - CC Evaluation of Assumptions for Multiple Linear Regression

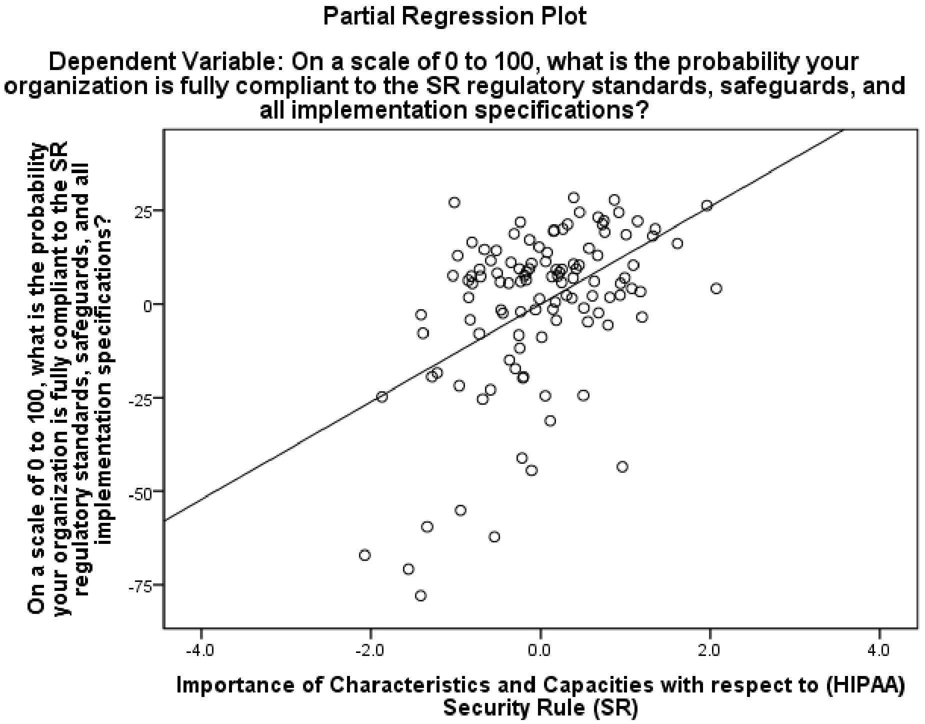


Figure R3. Characteristics and Capacities: Evaluating the Linearity assumption that the IV of CC individually have a linear relationship with the DV (PC1).

Appendix R: continued

MLR - RR Evaluation of Assumptions for Multiple Linear Regression

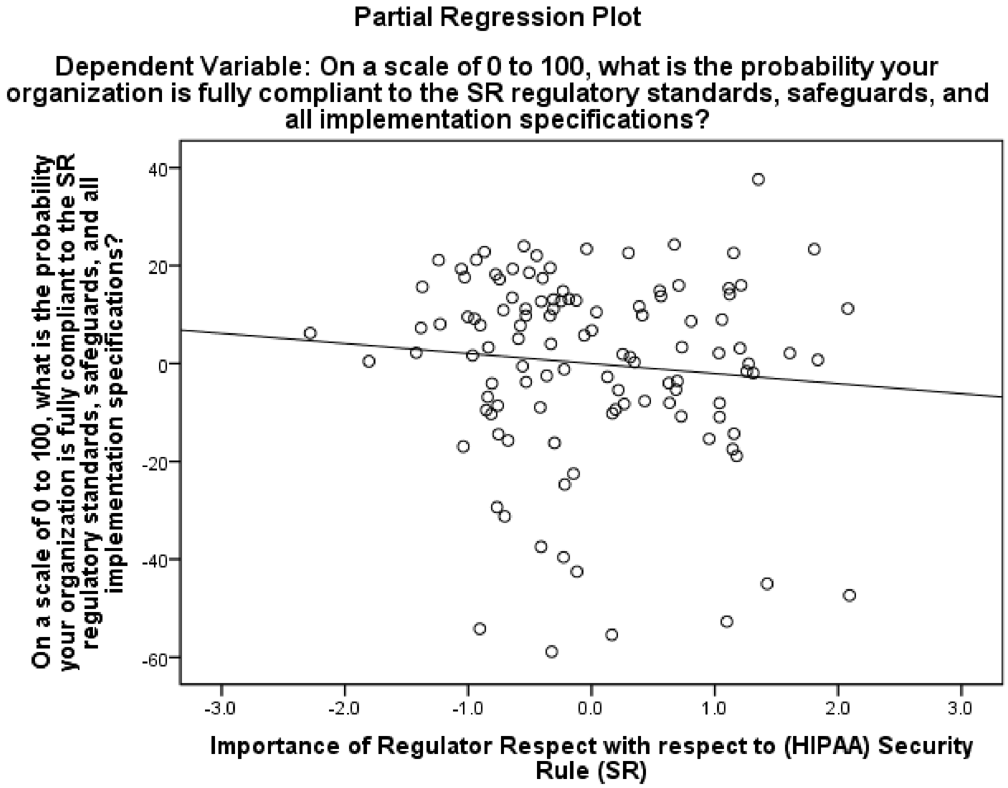


Figure R4. Regulator Respect: Evaluating the Linearity assumption that the IV of RR individually have a linear relationship with the DV (PC1).

Appendix R: continued

MLR - DT Evaluation of Assumptions for Multiple Linear Regression

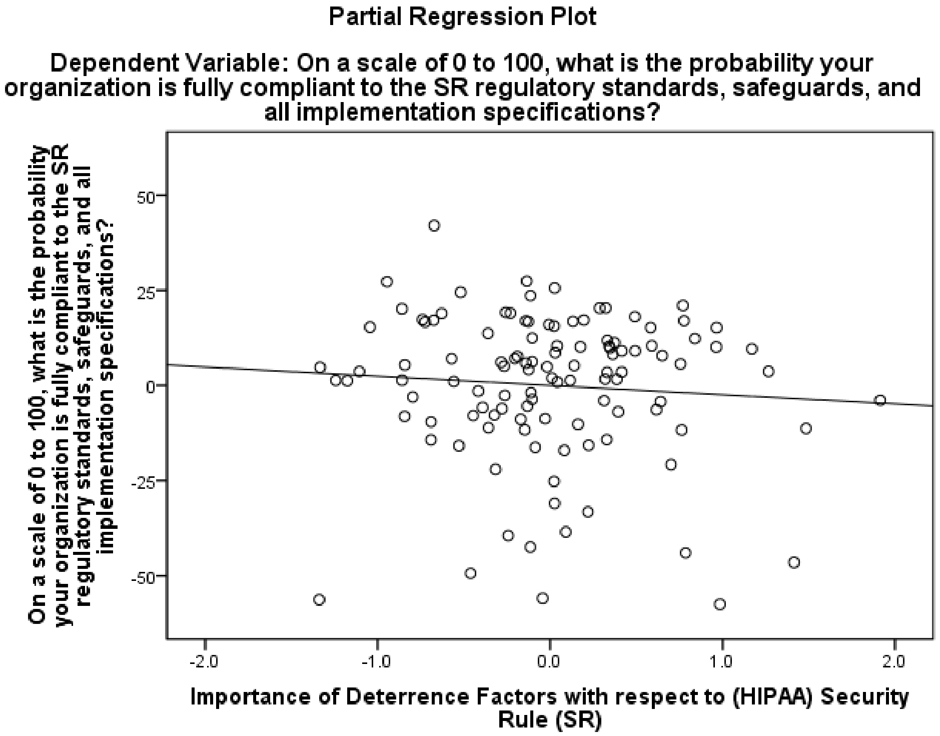


Figure R5. Deterrence Factors (DT): Evaluating the Linearity assumption that the IV of DT individually have a linear relationship with the DV (PC1).

Appendix S:

MLR - Evaluating the constant variance assumption.

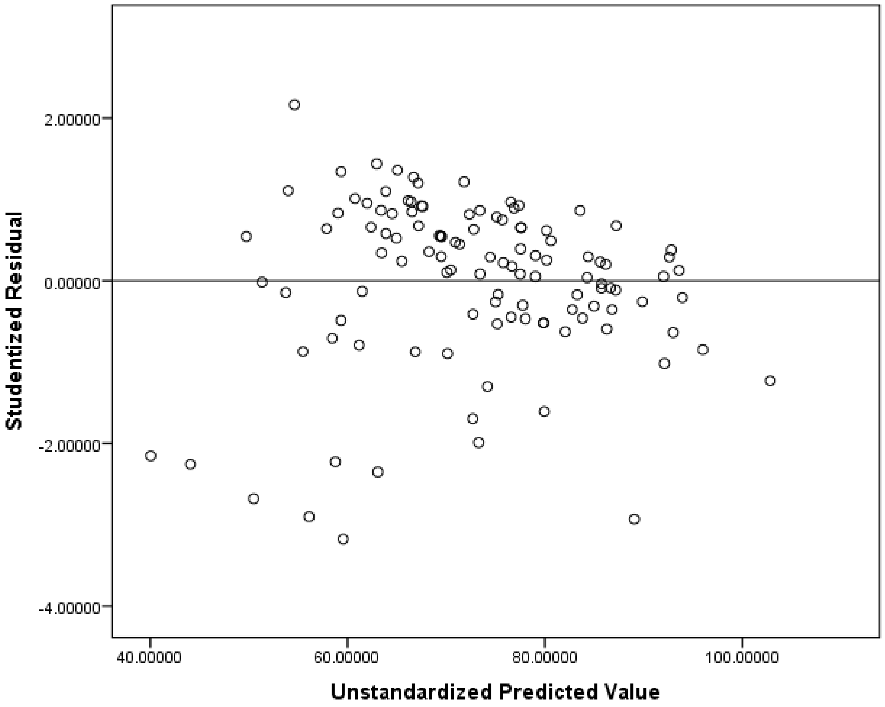


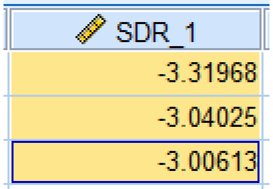
Figure S1. Evaluating the Constant Variance Assumption.

Appendix T:

MLR – Studentized Deleted Residuals, Leverage Values, and Cook's Values

Top 3 Deleted Residuals

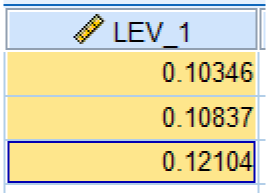
Three smallest Studentized Deleted Residuals to evaluate potential outliers.



SDR_1
-3.31968
-3.04025
-3.00613

Top 3 Leverage Values

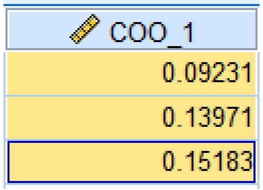
Three largest Leverage values to evaluate potential study participants that may adversely affect the regression parameter estimates.



LEV_1
0.10346
0.10837
0.12104

Cook's Distance Values

Three largest Cook's Distance values to evaluate potential, influential data points.



COO_1
0.09231
0.13971
0.15183

Appendix U:

Hypothesis 1 (H1) - Evaluation of Assumptions

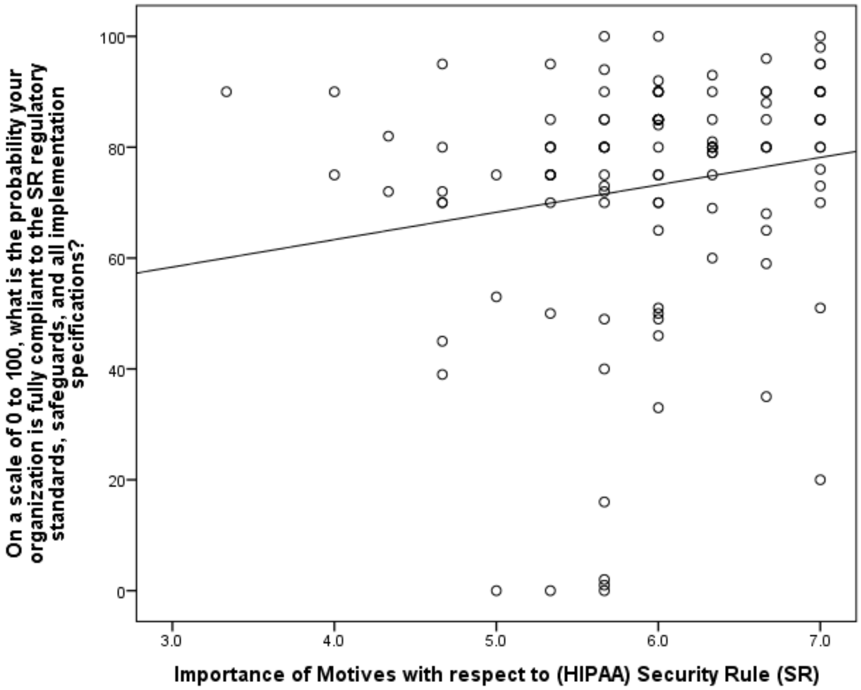


Figure U1. H1- Evaluating the Linearity and No Outliers Assumptions.

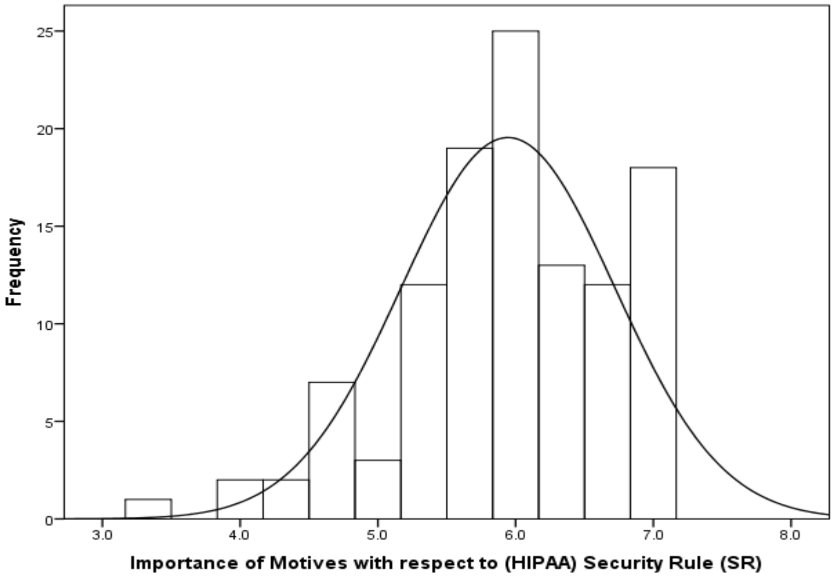


Figure U2. H1- Evaluating the Normality Assumption for the Motive Variable

Appendix U continued

Hypothesis 1 - Evaluation of Assumptions

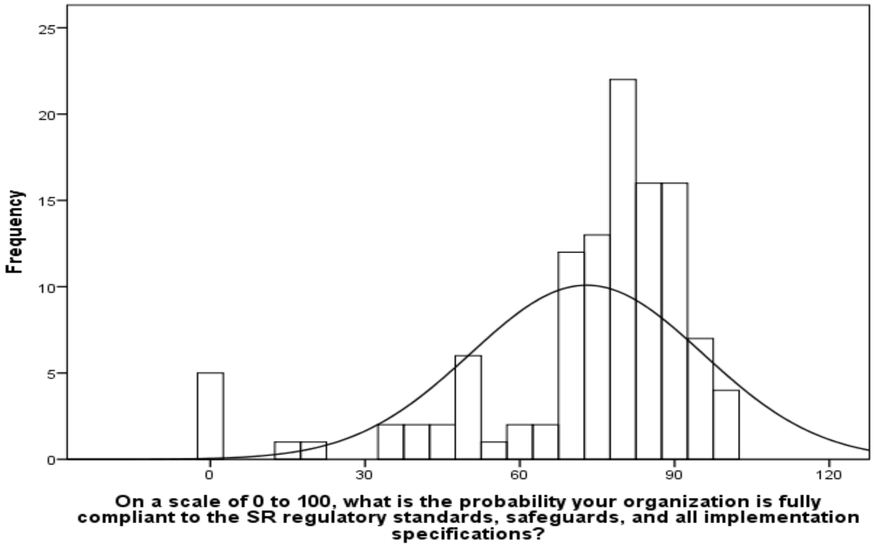


Figure U3. H1 - Evaluating the Normality Assumption for the PC1 Variable.

Appendix V:

Hypothesis 2 - Evaluation of Assumptions

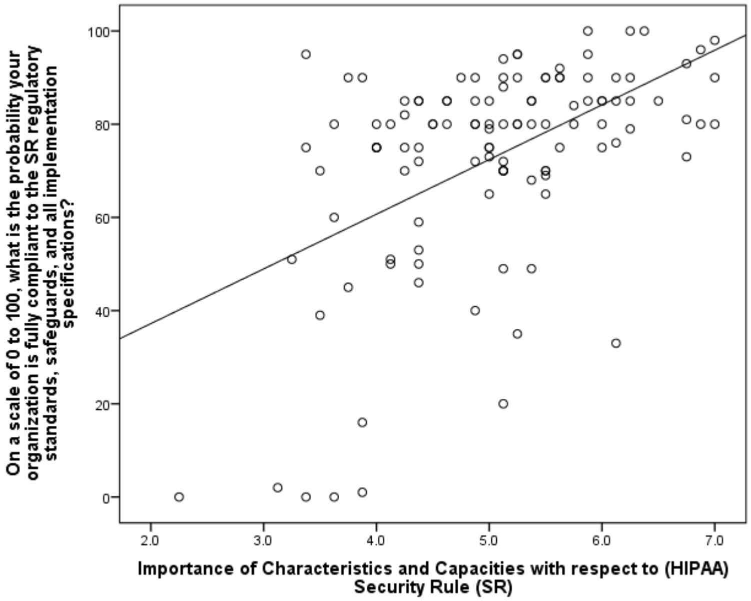


Figure V1. H2 - Evaluating the Linearity and No Outliers Assumptions.

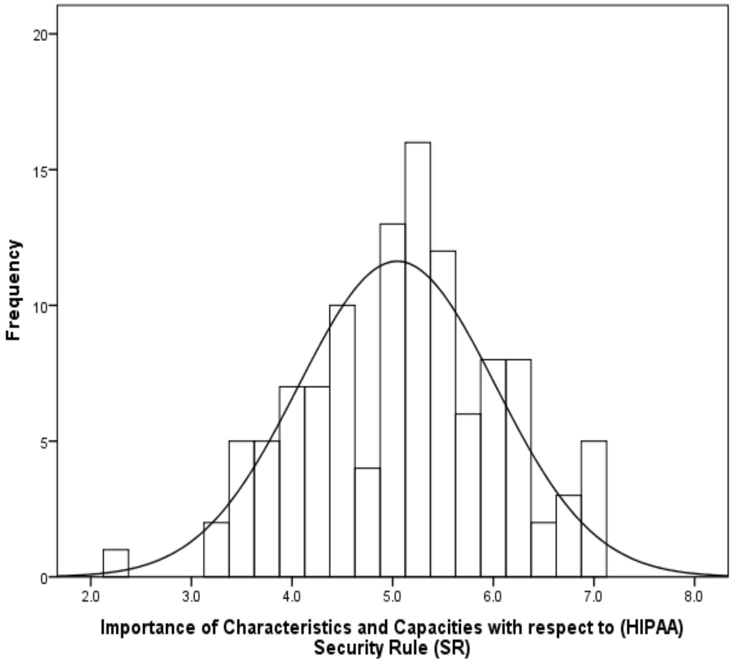


Figure V2. H2- Evaluating the Normality Assumption for the CC Variable.

Appendix V: continued

Hypothesis 2 - Evaluation of Assumptions

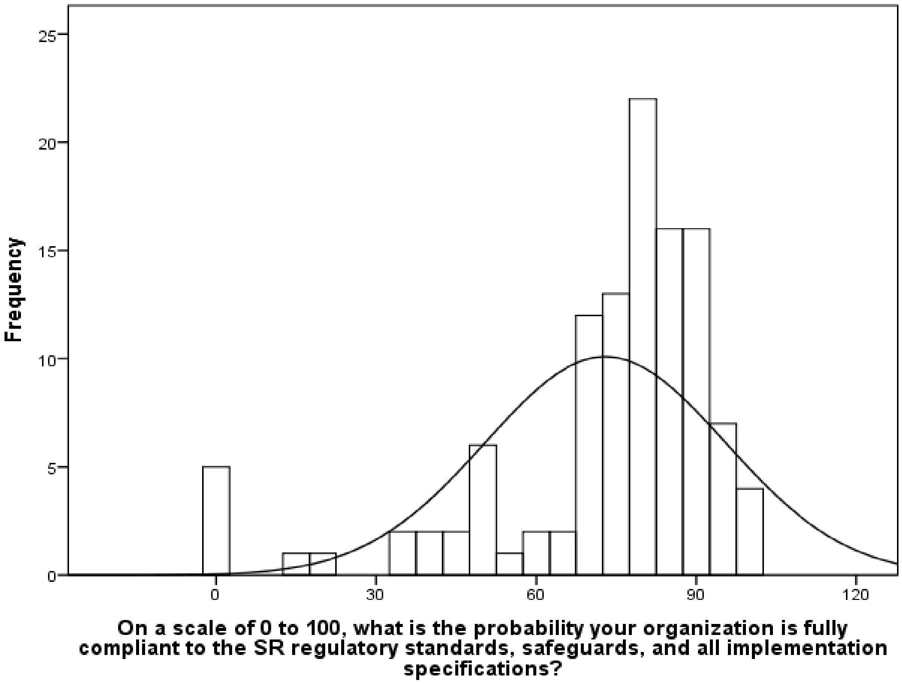


Figure V3. H2 - Evaluating the Normality Assumption for the PC1 Variable.

Appendix W:

Hypothesis 3 - Evaluation of Assumptions

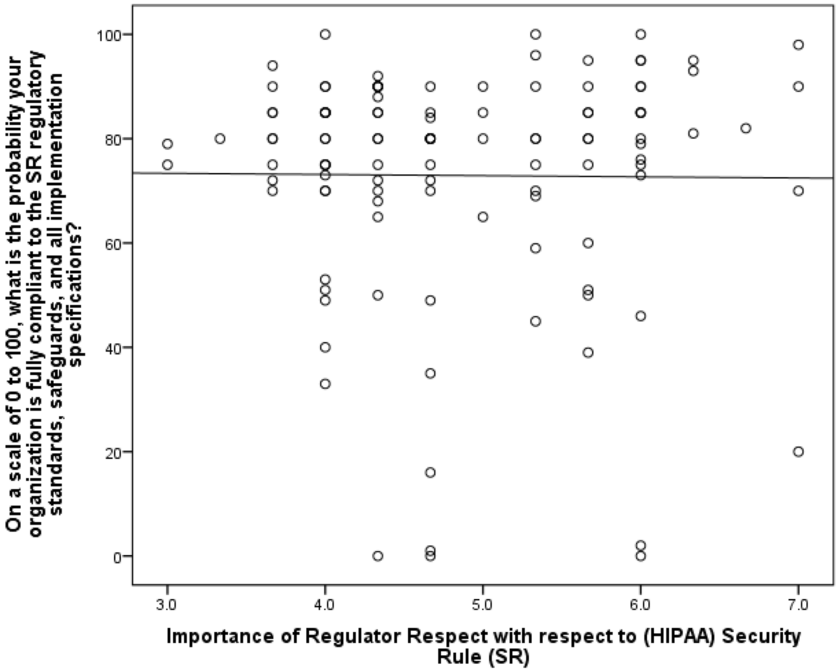


Figure W1. H3 - Evaluating the Linearity and No Outliers Assumptions.

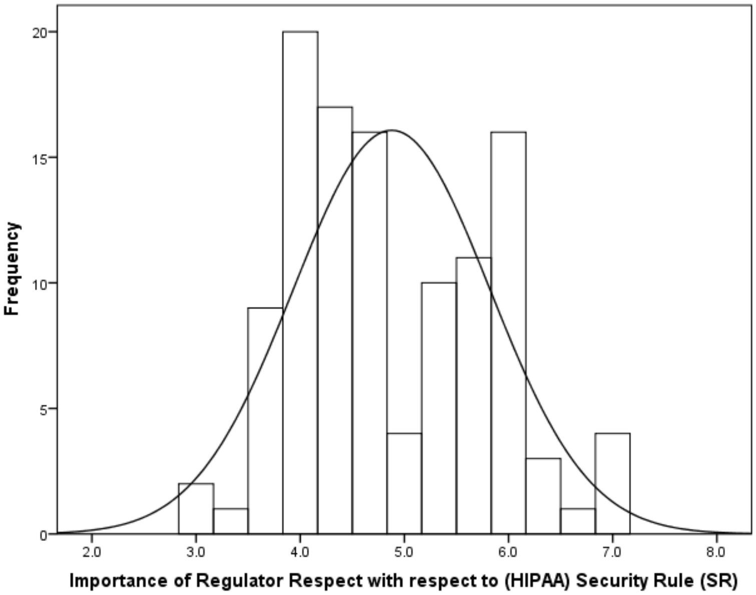


Figure W2. H3 - Evaluating the Normality Assumption for the RR Variable.

Appendix W: continued

Hypothesis 3 - Evaluation of Assumptions

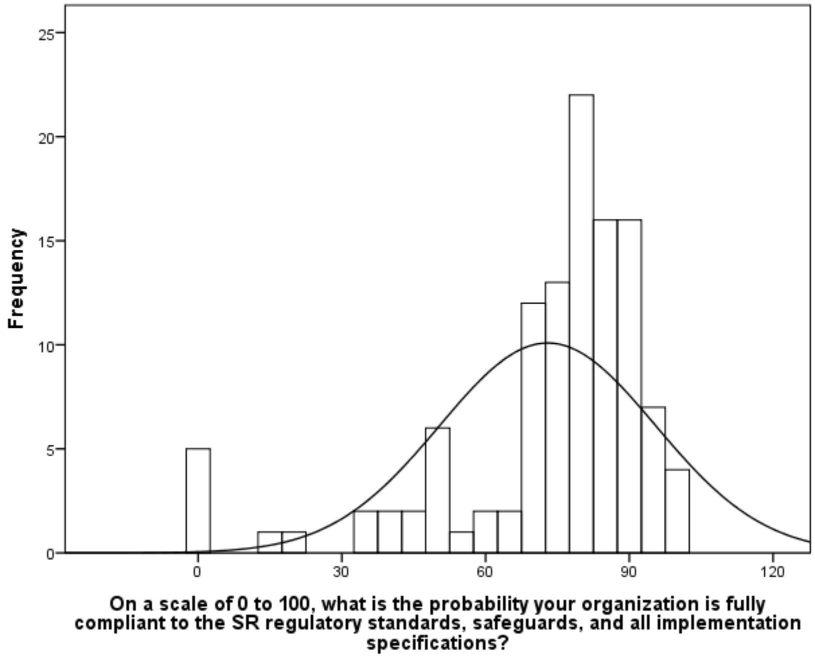


Figure W3. H3 - Evaluating the Normality Assumption for the PC1 Variable.

Appendix X:

Hypothesis 4 - Evaluation of Assumptions

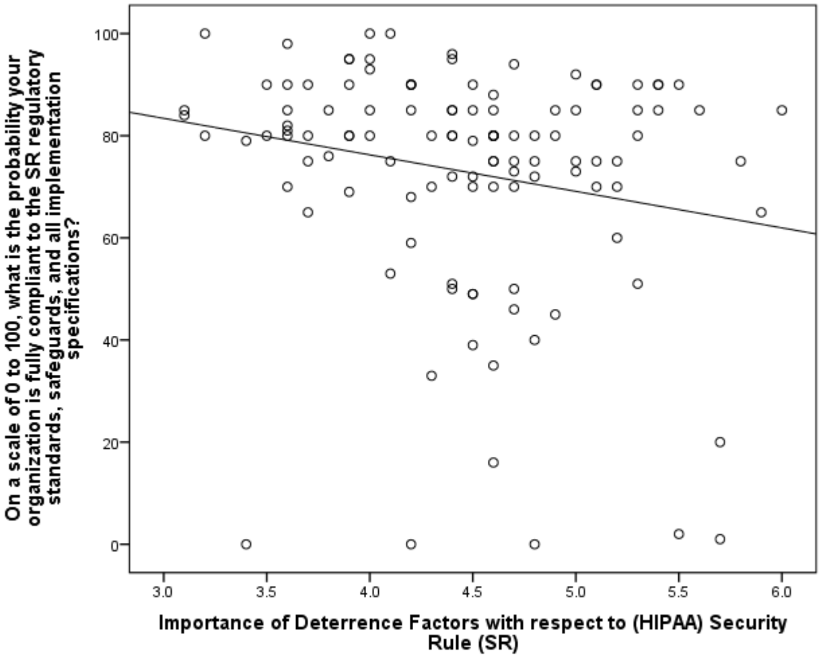


Figure X1. H4 - Evaluating the Linearity and No Outliers Assumptions.

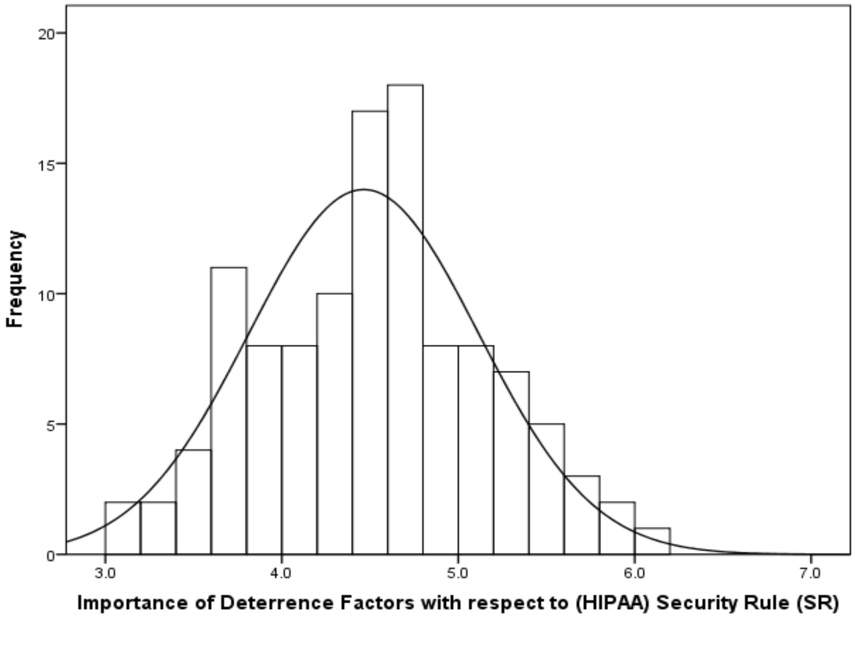


Figure X2. H4 - Evaluating the Normality Assumption for DT Variable

Appendix X: continued

Hypothesis 4 - Evaluation of Assumptions

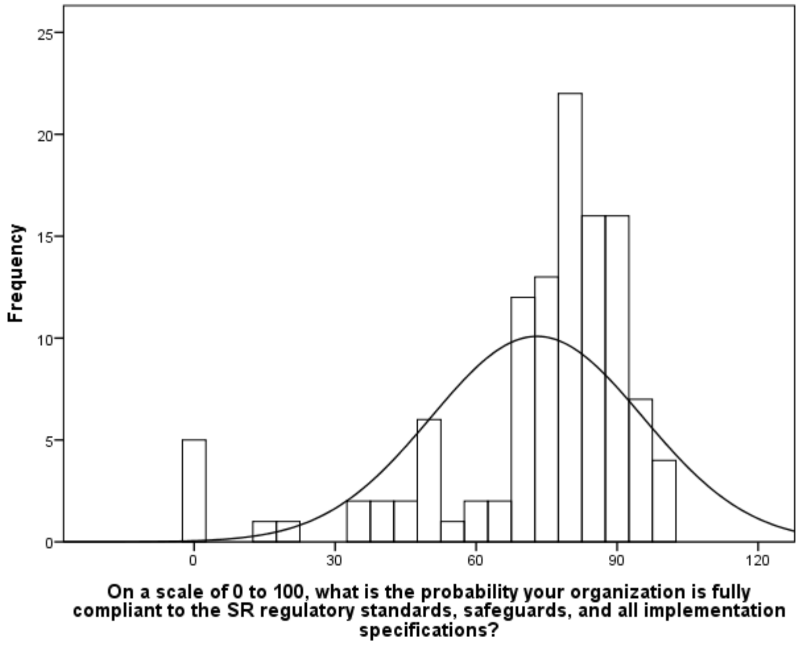


Figure X3. H4 - Evaluating the Normality Assumption for the PC1 Variable.

References

Ahmed, A., Hepu, D., Booi, K., & Xiaojuan, Z. (2017). Information security compliance in organizations: An institutional perspective, *1*(2), 104–114.

Akoglu, H. (2018). User's guide to correlation coefficients. *Turkish Journal of Emergency Medicine*. https://doi.org/10.1016/j.tjem.2018.08.001.

Al-Mukahal, H. M., & Alshare, K. (2015). An examination of factors that influence the number of information security policy violations in Qatari organizations. *Information and Computer Security*, *23*(1), 102–118. https://doi.org/10.1108/ICS-03-2014-0018.

Alder, S. (Ed). (2017). HIPAA compliance guide. *HIPAA Journal*. Retrieved from https://www.hipaajournal.com/wp-content/uploads/2015/05/HIPAAJournal-com-HIPAA-Compliance-Guide.pdf.

Alzahrani, A., Johnson, C., & Altamimi, S. (2018). Information security policy compliance: Investigating the role of intrinsic motivation towards policy compliance in the organization. In *2018 4th International Conference on Information Management (ICIM)* (pp. 125–132). https://doi.org/10.1109/INFOMAN.2018.8392822.

American National Standards Institute (ANSI). (2012). The Financial Impact of Breached Protected Health Information - A Business Case for Enhanced PHI Security.

Angst, C. M., Block, E. S., D 'Arcy, J., & Kelley, K. (2017). When do IT security investments matter? Accounting for the influence of institutional factors in the context of healthcare data breaches. *MIS Quarterly, 41*(3), 1–24. Retrieved from https://www3.nd.edu/~cangst/CoreyAngst_FacultyWebsite_files/Angst2017MISQSymbolicBreach.pdf.

Anthony, D. L., Appari, A., & Johnson, M. E. (2014). Institutionalizing HIPAA Compliance: Organizations and Competing Logics in U.S. Health Care. *Journal of Health and Social Behavior, 55*(1), 108–124, https://doi.org/10.1177/0022146513520431.

Appari, A., Anthony, D. L., & Johnson, M. E. (2006). Which Hospitals Are Complying with HIPAA: An Empirical Investigation of US Hospitals, (2006), 1–18.

Appari, A., Anthony, D. L., & Johnson, M. E. (2009). HIPAA Compliance: An Examination of Institutional and Market Forces. *Proceedings of the 8th Workshop on Economics of Information Security*, (2006), 1–23.

Appari, A., & Johnson, M. E. (2010). Information security and privacy in healthcare: current state of research. *International Journal of Internet and Enterprise*

Management, *6*(4), 279–314. Retrieved from https://www.inderscience.com/jhome.php?jcode=ijiem#journalDetail.

Aron, A., Coups, E., & Aron, E. (2017). *Statistics for Psychology*. *Statistics for Psychologists* (7th ed.). Boston: Pearson Boston, MA. https://doi.org/978-0-205-25815-4.

Asmonga, D., Burrington-Brown, J., Jill, R., Dennis, C., Fiorio, S., Gould, K., … Zender, A. (2004). The state of HIPAA privacy and security compliance, 1–38. Retrieved from https://library.ahima.org/PdfView?oid=23016.

Avella, J. R. (2016). Delphi panels: Research design, procedures, advantages, and challenges. *International Journal of Doctoral Studies*, *11*, 305–321. https://doi.org/10.28945/3561.

Bagozzi, R. P. (2011). Measurement and meaning in information systems and organizational research: Methodological and philosophical foundations, *35*(2), 261–292.

Beaver, K. (2018). HIPAA security compliance fallacies (And how to avoid them). Retrieved from https://blog.rapid7.com/2018/02/12/hipaa-security-compliance-fallacies-and-how-to-avoid-them/.

Benitez, K., & Malin, B. (2010). Evaluating re-identification risks with respect to the HIPAA privacy rule. *Journal of the American Medical Informatics Association*, *17*(2), 169–177. https://doi.org/10.1136/jamia.2009.000026.

Bilimoria, N. M. (2009). HIPAA Privacy/Security Rules: Where We’ve Been and Where We Are Going Updates. *Medical Practice Management*, 149–152. Retrieved from https://www.duanemorris.com/articles/static/bilimoria_mpm_1109.pdf.

Blackbook Market Research LLC. (2018). State of the healthcare IT and data security industry: 2018 user survey results, (May), 1–65. Retrieved from https://cdn.newswire.com/files/x/4f/22/7372928feb8ec9258897b7863dd4.pdf.

Brady, J. W. (2010). An investigation of factors that affect HIPAA security compliance in academic medical centers. Retrieved from https://nsuworks.nova.edu/gscis_etd/100/.

Brinkman, E. (2019). HIPAA Privacy : Liability beyond regulatory enforcement.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523–548. https://doi.org/10.1093/bja/aeq366.

Bulgurcu, B., Cavusoglu, H., & Izak, B. (2010). Information security policy compliance: An empirical study of rationality-based beliefs. *MIS Quarterly*, *34*(3), 523–548.

Retrieved from http://www.jstor.org/stable/25750690.

Burch, P., & Heinrich, C. (2016). *Mixed methods for policy research and program evaluation* (1st ed.). Thousand Oaks, California: SAGE Publications Inc.

Cannoy, S. D., & Salam, A. F. (2010). A framework for health care information assurance policy and compliance. *Communications of the ACM*, *53*(3), 126. https://doi.org/10.1145/1666420.1666453.

Cenfetelli, R., Bassellier, G., Cenfetelli, B. R. T., & Bassellier, G. (2009). Interpretation of Formative Measurement in Information Systems Research. *MIS Quarterly*, *33*(4), 689–707. https://doi.org/Article.

Charmaz, K. (2000). Grounded theory: Objectivist and constructivist methods. *Handbook of Qualitative Research*, *2*, 509–535.

Chen, J., & Benusa, A. (2017). HIPAA security compliance challenges: The case for small healthcare providers. *International Journal of Healthcare Management*, *10*, 135–146. https://doi.org/10.1080/20479700.2016.1270875.

Chen, X., Wu, D., Chen, L., & Teng, J. K. L. (2018). Sanction severity and employees' information security policy compliance: Investigating mediating, moderating, and control variables. *Information & Management*, *55*(8), 1049–1060. https://doi.org/https://doi.org/10.1016/j.im.2018.05.011.

Clearwater Compliance LLC. (2019). Key Takeaways From Breakfast & Breaches. Retrieved November 22, 2019, from https://clearwatercompliance.com/blog/key-takeaways-from-breakfast-breaches-d-c/.

CMMS Medicaid Services. (2009). HIPAA Compliance Review Analysis and Summary of Results.

Cogan, J. A. (2005). First ever HIPAA conviction highlights differing views of HIPAA's civil and criminal penalties. *Rhode Island Medical Journal*, *88*(1), 33–34. Retrieved from https://search-proquest-com.ezproxylocal.library.nova.edu/central/docview/195803905/fulltextPDF/2BD00EBDA4654424PQ/1?accountid=6579.

Cohen, G., & Mello, M. (2018). HIPAA and protecting health information in the 21st century. *JAMA*, *320*(3), 231–232. https://doi.org/10.1001/jama.2018.5630.

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2nd ed.). New York, New York: Lawrence Erlbaum Associates.

Cohen, L. T. (2016). Office for Civil Rights HIPAA enforcement actions provide valuable insight to radiologists. *Journal of the American College of Radiology*, *13*, 666–667. https://doi.org/10.1016/j.jacr.2016.03.007.

Cook, R. D. (1977). Detection of influential observation in linear regression. *Technometrics*, *19*(1), 15–18.

Creech, S. (2016). *Why should I perform Pearson's Correlation and Multiple Linear Regression Analysis*?

Creswell, J. W. (2019). *Educational Research* (6th ed.). Upper Saddle River, N.J.: Pearson/Merrill Prentice Hall.

Creswell, J. W., & Creswell, D. J. (2018a). Cresswell choosing a mixed methods design, 58–89. https://doi.org/1412927927.

Creswell, J. W., & Creswell, D. J. (2018b). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). Thousand Oaks, CA: SAGE Publications Inc.

Creswell, J. W., & Guetterman, T. (2019). *Educational research: Planning, conducting, and evaluating quantitative and qualitative research* (6th ed.). New York, NY: Pearson.

Crumpler, W., & Lewis, J. A. (2019). The Cybersecurity workforce gap. *Center for Strategic and International Studies*, 1–10. Retrieved from http://www.isaca.org/Knowledge-Center/.

Dalkey, N., & Helmer, O. (1963). An experimental application of the Delphi method to the use of experts. *Management Science*, *9*(3), 458–467. Retrieved from http://www.jstor.org/stable/2627117.

Danermark, B., Ekstrom, M., & Jakobsen, L. (2005). *Explaining society: An introduction to critical realism in the social sciences*. Routledge.

Davis, J. (2019). West Georgia Ambulance Pays $65K OCR Settlement for HIPAA Violations. Retrieved January 7, 2020, from https://healthitsecurity.com/news/west-georgia-ambulance-pays-65k-ocr-settlement-for-hipaa-violations?eid=CXTEL000000084795&elqCampaignId=12875&utm_source=nl&utm_medium=email&utm_campaign=newsletter&elqTrackId=c43fcc8b409c485694015ecec22cb29d&elq=f9fab15c.

Davis, J. (2020). Cyber Threats Behind the Biggest Healthcare Data Breaches of 2019. Retrieved January 7, 2020, from https://healthitsecurity.com/news/cyber-threats-behind-the-biggest-healthcare-data-breaches-of-2019?eid=CXTEL000000084795&elqCampaignId=12875&utm_source=nl&utm_medium=email&utm_campaign=newsletter&elqTrackId=2d2bdcd9d5f74440ac79fe3c8a26c0fd&elq=f9fab15c9b.

Demartine, A., Pollard, J., Blankenship, J., Cser, A., Shey, H., Mcclean, C., … Maxim, M. (2016). *Predictions 2017 : Cybersecurity Risks Intensify*. *Forrester*.

Demidenko, E. (2007). Sample size determination for logistic regression revisited. *Statistics in Medicine*, *26*(18), 3385–3397. https://doi.org/10.1002/sim.2771

Dhakal, C. (2018). Interpreting the basic outputs (SPSS) of multiple linear regression. *International Journal of Science and Research (IJSR)*. https://doi.org/10.21275/4061901.

Donavan, F. (2018). HIPAA security rule risk analysis remains source of confusion. *HealthITSecurity*. Retrieved from https://healthitsecurity.com/news/hipaa-security-rule-risk-analysis-remains-source-of-confusion?

Drahos. (2017a). *Regulatory Theory*. (P. Drahos, Ed.). ANU Press. Retrieved from http://www.jstor.org/stable/j.ctt1q1crtm.

Drahos, P. (2017b). Regulatory globalization. In P. Drahos (Ed.), *Regulatory Theory* (pp. 249–264). ANU Press. Retrieved from http://www.jstor.org/stable/j.ctt1q1crtm.24.

Drahos, P. (2017c). *Regulatory Theory: Foundations and Applications*. Retrieved from http://press-files.anu.edu.au/downloads/press/n2304/pdf/book.pdf?referer=2304.

Drahos, P., & Krygier, M. (2017). Regulation, institutions, and networks. In P. Drahos (Ed.), *Regulatory Theory* (pp. 1–22). ANU Press. Retrieved from http://www.jstor.org/stable/j.ctt1q1crtm.7.

Drolet, B. C., Marwaha, J. S., Hyatt, B., Blazar, P. E., & Lifchez, S. D. (2017). Electronic Communication of Protected Health Information: Privacy, Security, and HIPAA Compliance. *The Journal of Hand Surgery*, *42*(6), 411–416. https://doi.org/10.1016/j.jhsa.2017.03.023.

Duncan, B., & Whittington, M. (2014). Compliance with standards, assurance and, audit. In *Proceedings of the 7th International Conference on Security of Information and Networks - SIN '14* (pp. 77–84). https://doi.org/10.1145/2659651.2659711.

Egress Software Technologies Ltd. (2019). *Insider Data Breach survey 2019*. Retrieved from https://pages.egress.com/InsiderDataBreachsurvey2019US.html.

Ellis, T. J., & Levy, Y. (2009). Towards a Guide for Novice Researchers on Research Methodology: Review and Proposed Methods. *Issues in Informing Science and Information Technology*, *6*, 323–337.

Fan, W., & Yan, Z. (2009). Factors affecting response rates of the web survey: A systematic review. https://doi.org/10.1016/j.chb.2009.10.015.

Field, A. (2017). *Discovering Statistics Using IBM SPSS Statistics* (5th ed.). SAGE Publications Inc.

Fortinet. (2018). Cybersecurity, cybercrime and data breaches: Healthcare under attack.

CSO Online. Retrieved from https://www.csoonline.com/article/3260191/security/healthcare-experiences-twice-the-number-of-cyber-attacks-as-other-industries.html.

Fowler, F. (2014). *Survey Research Methods* (5th ed.). Thousand Oaks, CA: SAGE Publications Inc.

Frost, J. (2017). How to interpret R-squared in regression analysis. Retrieved fromhttp://statisticsbyjim.com/regression/interpret-r- squared-regression/ Accessed on 11 March 2020.

G. Stoneburner, Goguen, A., & Feringa, A. (2002). Risk management guide for information technology systems. *National Institute of Standards and Technology, Special Publication 800 -30, 800–30*, 55. https://doi.org/10.1111/j.1745-6622.2008.00202.x.

Gaia, J., Wang, X., Basile, J., Sanders, G. L., & Murray, D. (2018). A study of factors in HIPAA non-compliant behavior. *Americas Conference on Information Systems 2018: Digital Disruption, AMCIS 2018*, 1–10. Retrieved from https://www.scopus.com/inward/record.uri?eid=2-s2.0-85054256663&partnerID=40&md5=4740b1575121b9a114911707cdc8f3bb.

Gallagher, A. (2016). HHS issues new HIPAA privacy, security, and breach notification audit protocol. Retrieved from https://www.ajg.com/media/1699426/technical-bulletin-2016-issue-6-hhs-issues-new-hipaa-audit-protocol-final.pdf.

Gideon, R. A., & Hollister, R. A. (1987). A rank correlation coefficient resistant to outliers. *Journal of the American Statistical Association*, *82*(398), 656–666. https://doi.org/10.1080/01621459.1987.10478480.

Gold, J. A., & Trudell, B. (2015). MetaStar Security Risk Assessments: HIPAA and Meaningful Use. *WMJ*.

Gold, M., & McLaughlin, C. (2016). Assessing HITECH implementation and lessons: 5 years later. *The Milbank Quarterly*, *94*(3), 654–687. Retrieved from http://www.jstor.org/stable/24869193.

Gunningham, N. (2010). Enforcement and compliance strategies. *The Oxford Handbook of Regulation*, *120*, 131–135.

Haines, F. (2017). Regulation and risk. In P. Drahos (Ed.), *Regulatory Theory* (pp. 181–196). ANU Press. Retrieved from http://www.jstor.org/stable/j.ctt1q1crtm.19.

Hash, J., Bowen, P., Johnson, A., Smith, C. D., Steinberg, D. I., & Gutierrez, C. M. (2008). An Introductory resource guide for implementing the Health Insurance Portability and Accountability Act (HIPAA) security rule. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-66/rev-1/final.

Hawthorne, K. H., & Richards, L. (2017). Personal health records: a new type of electronic medical record. *Records Management Journal*, *27*(3), 286–301. https://doi.org/10.1108/RMJ-08-2016-0020.

Health Insurance Portability and Accountability Act (HIPAA). (1996). 45 CFR 160.103, 979–974.

Healthcare Information and Management Systems Society (HIMSS). (2018). 2018 HIMSS cybersecurity survey. Retrieved from https://www.himss.org/sites/himssorg/files/u132196/2018_HIMSS_Cybersecurity_Survey_Final_Report.pdf.

Healthcare Information and Management Systems Society (HIMSS). (2019). 2019 HIMSS Cybersecurity Survey. Retrieved from https://www.himss.org/sites/himssorg/files/u132196/2019_HIMSS_Cybersecurity_Survey_Final_Report.pdf.

HIMSS Analytics. (2019). The Dorenfest Institute for Health Information. Retrieved June 7, 2019, from https://foundation.himss.org/Dorenfest.

HIPAA Journal. (2017). OCR HIPAA enforcement: Summary of 2016 HIPAA settlements. *HIPAA Journal*. Retrieved from https://www.hipaajournal.com/ocr-hipaa-enforcement-summary-2016-hipaa-settlements-8646/.

Hoffman, S., & Podgurski, A. (2006). Securing the HIPAA security rule. *Journal of Internet Law*, *10*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=953670.

Holtzman, D. (2017). OCR releases phase 2 HIPAA audits preliminary results. Retrieved from https://cynergistek.com/blog/ocr-desk-audits-preliminary-results/.

Johnson, R. B., Onwuegbuzie, A. J., & Turner, L. A. (2007). Toward a definition of Mixed Methods research. *Journal of Mixed Methods Research*, *1*(2), 112–133. https://doi.org/10.1177/1558689806298224.

Johnston, A. C., & Warkentin, M. (2008). Information privacy compliance in the healthcare industry. *Information Management & Computer Security*, *16*(1), 5–19. https://doi.org/10.1108/09685220810862715.

Kieser, M., & Wassmer, G. (1996). On the Use of the Upper Confidence Limit for the Variance from a Pilot Sample for Sample Size Determination. *Biometrical Journal*, *38*(8), 941–949. https://doi.org/10.1002/bimj.4710380806.

Kingsbury, B. (1997). The concept of compliance as a function of competing conceptions of international law. *Mich. J. Int'l L.*, *19*, 345.

Kuo, K. M., Chen, Y. C., Talley, P. C., & Huang, C. H. (2018). Continuance compliance of privacy policy of electronic medical records: the roles of both motivation and habit. *BMC Medical Informatics and Decision Making*, *18*(1), 135. https://doi.org/10.1186/s12911-018-0722-7.

Laerd Statistics LLC. (2019). Multiple regression in SPSS Statistics. Retrieved January 6, 2020, from https://statistics.laerd.com/premium/spss/mr/multiple-regression-in-spss-16.php.

Lane, D. (n.d.). *Online Statistics Education: An Interactive Multimedia Course of Study*. Houston, Texas: Rice University. Retrieved from http://onlinestatbook.com/2/regression/influential.html.

Leedy, P. D. (2016). *Practical Research* (Vol. 11). Upper Saddle River, N.J.: Pearson.

Leedy, P., & Ormrod, J. (2019). *Practical research: Planning and design*. New York, N.Y.: Pearson Education, Inc.

Levy, Y., & Ellis, T. J. (2006). A systems approach to conduct an effective literature review in support of information systems research. *Informing Science: International Journal of an Emerging Transdiscipline*, *9*, 181–212.

Liginlal, D., Sim, I., Khansa, L., & Fearn, P. (2012). HIPAA Privacy Rule compliance: An interpretive study using Norman's action theory. *Computers and Security*, *31*(2), 206–220. https://doi.org/10.1016/j.cose.2011.12.002.

Lisbon, S., & Rice, E. (2015). Case study : Information security risk assessment for a small healthcare clinic using the security risk assessment tool. Retrieved from http://www.micsymposium.org/mics_2017_proceedings/docs/MICS_2017_paper_7.pdf.

Litten, E. G. (2017). HIPAA audit preparedness. Retrieved from https://www.hcca-info.org/Portals/0/PDFs/Resources/Conference_Handouts/Regional_Conference/2017/new-york/Littenprint2.pdf.

Liu, C., Milton, J., & McIntosh, A. (2016). Regression Diagnostics. Retrieved December 24, 2019, from http://sphweb.bumc.bu.edu/otlt/MPH-Modules/BS/R/R5_Correlation-Regression/R5_Correlation-Regression7.html.

Losoncz, I. (2017). Methodological approaches and considerations in regulatory research. In P. Drahos (Ed.), *Regulatory Theory* (pp. 77–96). ANU Press. Retrieved from http://www.jstor.org/stable/j.ctt1q1crtm.12.

Martin, N. L., Imboden, T., & Green, D. T. (2015). HIPAA security rule compliance in small healthcare facilities: theoretical framework. *Issues in Information Systems, 16*(1), 180–188. Retrieved from http://www.iacis.org/iis/2015/1_iis_2015_180-188.pdf.

Martin, N. L., & Imboden, T. R. (2014). Information security and insider threats in small medical practices. *Twentieth Americas Conference on Information Systems*, 1–9. Retrieved from https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1614&context=amcis2014.

McLeod, A., & Dolezel, D. (2018). Cyber-analytics: Modeling factors associated with healthcare data breaches. *Decision Support Systems*, *108*, 57–68. https://doi.org/10.1016/j.dss.2018.02.007.

McMillan, M. (2015). Is it time to revisit the HIPAA security rule? Retrieved from https://cynergistek.com/time-revisit-the-hipaa-security-rule/.

Mertler, C. A., & Reinhart, R. V. (2016). *Advanced and Multivariate Statistical Methods* (6th ed.). Routledge.

Miaou, S. P., Lu, A., & Lum, H. S. (1996). Pitfalls of using R2 to evaluate goodness of fit of accident prediction models. Transportation Research Record, (1542), 6–13. https://doi.org/10.3141/1542-02.

Mohammed, D., Mariani, R., & Mohammed, S. (2015). Cybersecurity challenges and compliance issues within the U.S. healthcare sector. *International Journal of Business and Social Research*, *5*(2), 55–66. Retrieved from http://www.thejournalofbusiness.org/index.php/site.

Mukaka, M. M. (2012). Statistics corner: A guide to appropriate use of correlation coefficient in medical research. *Malawi Medical Journal*, *24*(3), 69–71.

Nardi, P. (2018a). *Doing Survey Research,* (4th ed.). New York, N.Y.: Routledge.

Nardi, P. (2018b). *Doing Survey Research* (4th ed.). Routledge.

Nielsen, V., & Parker, C. (2012). Mixed motives: Economic, social, and normative motivations in business compliance. *Law & Policy*, *34*(4), 428–462. https://doi.org/10.1111/j.1467-9930.2012.00369.x.

O’Brien, R. M. (2007). A caution regarding rules of thumb for variance inflation factors. *Quality and Quantity*, *41*(5), 673–690. https://doi.org/10.1007/s11135-006-9018-6.

Okoli, C., & Pawlowski, S. D. (2004). The Delphi method as a research tool: An example, design considerations and applications. *Information & Management*, *42*, 15–29. https://doi.org/10.1016/J.IM.2003.11.002.

Osborne, J. W., & Waters, E. (2002). Four assumptions of multiple regression that researchers should always test. *Practical Assessment, Research and Evaluation*, *8*(2), 1–5. Retrieved from http://pareonline.net/getvn.asp?n=2&v=8.

Parker, C., & Nielsen, V. (2017). Compliance: 14 questions. In P. Drahos (Ed.), *Regulatory Theory* (pp. 217–232). ANU Press. Retrieved from http://www.jstor.org/stable/j.ctt1q1crtm.21.

Parker, C., & Nielsen, V. L. (2010). The challenge of empirical research on business Compliance in regulatory capitalism. *Ssrn*, 45–70. https://doi.org/10.1146/annurev.lawsocsci.093008.131555.

Parker, C., & Nielsen, V. L. (2011). *Explaining compliance: Business responses to regulation*. Edward Elgar Publishing, Incorporated. Retrieved from https://books.google.com/books?id=e4Icg5ymiz8C.

Parker, C. (1999). Compliance Professionalism and Regulatory Community: The Australian Trade Practices Regime. *Journal of Law and Society*, *26*(2), 215–239. Retrieved from http://www.jstor.org/stable/1410497.

Parker, C., & Nielsen, V. L. (2009). Corporate compliance systems: Could they make any difference? *Administration & Society*, *41*(1), 3–37.

Parker, C., & Nielson, V. L. (2006). Do businesses take compliance systems seriously-an empirical study of the implementation of trade practices compliance systems in Australia. *Melb. UL Rev.*, *30*, 441.

Plummer, J. D., & Tanis Ozcelik, A. (2015). Preservice Teachers Developing Coherent Inquiry Investigations in Elementary Astronomy. *Science Education*, *99*(5), 932–957. https://doi.org/10.1002/sce.21180.

Ponemon Institute. (2016). Sixth annual benchmark study on privacy and security of healthcare data, (May). Retrieved from http://www.ponemon.org/local/upload/file/Sixth Annual Patient Privacy %26 Data Security Report FINAL 6.pdf.

Ponemon Institute. (2019). Cost of a data breach report, 76. Retrieved from https://www.ibm.com/downloads/cas/ZBZLY7KL.

Price Waterhouse Cooper. (2016). Global State of Information Security Survey 2016.

Primeau, & Debra. (2017). How small organizations handle HIPAA compliance. *Journal of AHIMA*, *88*(4), 18–21. Retrieved from http://bok.ahima.org/doc?oid=302074.

Ramim, M. M., & Lichvar, B. T. (2014). Eliciting expert panel perspective on effective collaboration in system development projects. *Online Journal of Applied Knowledge Management*, *2*(1), 122–136.

Ramsey, P. H. (1989). *Critical Values for Spearman's Rank Order Correlation*. *Source: Journal of Educational Statistics* (Vol. 14).

Redspin. (2016). *Breach Report 2016:Protected Health Information (PHI)*. Retrieved from https://www.redspin.com/resources/download/breach-report-2016-protected-health-information-phi/.

Reis, D. W. (2012). *An Examination of an Information Security Framework Implementation Based on Agile Values to Achieve Health Insurance Portability and Accountability Act Security Rule Compliance in an Academic Medical Center*. Nova Southeastern University.

Robinson, G., & Mcneill, F. (2012). Theoretical Criminology Exploring the dynamics of compliance with community penalties, *12*(June). https://doi.org/10.1177/1362480608097151.

Robinson, S. (2019). *Designing Quality Survey Questions*. SAGE Publications Inc.

Rodriguez, L. (2013). *Dialogue on HIPAA / HITECH compliance resolution agreement with Idaho State University*. Retrieved from https://csrc.nist.gov/CSRC/media/Presentations/HIPAA-2013-Dialogue-on-HIPAA-HITECH-Compliance/images-media/rodriguez_leon_day2_900_dialogue_on_hipaa.pdf%0A%0A.

Ruel, E. (2018). *100 questions (and answers) about survey research* (First). Thousand Oaks: SAGE Publications Inc.

Ruel, E., Wagner, E., & Gillespie, J. (2016). *Pretesting and Pilot Testing 101*. SAGE Publications Inc.

SAI Global. (2017). 2017 Healthcare compliance benchmark study, 1–12.

Sanches, L. (2017). Update on audits of entities compliance with the HIPAA rules. Retrieved from https://cynergistek.com/wp-content/uploads/2017/09/OCR-CE-Desk-Audit-Results-09_17-.pdf.

Shindell, R. (2016). HIPAA privacy and security compliance: Survey results. Retrieved from https://www.todayswoundclinic.com/articles/hipaa-privacy-security-compliance-survey-results.

Sittig, D. F., Belmont, E., & Singh, H. (2017). Improving the safety of health information technology requires shared responsibility: It is time we all step up. *Healthcare*, *6*, 7–12. https://doi.org/10.1016/j.hjdsi.2017.06.004.

Sohrabi Safa, N., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers and Security*, *56*, 1–13. https://doi.org/10.1016/j.cose.2015.10.006.

Stevens, G. (2009). Enforcement of HIPAA privacy and security rules. *Congressional Research Service*.

Studenmund, A. (2017). *Using Econometrics: A Practical Guide* (7th ed.). Pearson Boston, MA.

Such, J. M., Gouglidis, A., Knowles, W., Misra, G., & Rashid, A. (2016). Information assurance techniques: Perceived cost effectiveness. *Computers and Security*, *60*, 117–133. https://doi.org/10.1016/j.cose.2016.03.009.

SurveyMonkey. (2019). Making responses anonymous. Retrieved April 5, 2019, from https://help.surveymonkey.com/articles/en_US/kb/How-do-I-make-surveys-anonymous.

Tabachnick, B. G., & Fidell, L. S. (2019). *Using multivariate statistics* (Vol. 7). Pearson Boston, MA.

Taber, K. S. (2018). The Use of Cronbach's Alpha When Developing and Reporting Research Instruments in Science Education. *Research in Science Education*, *48*(6), 1273–1296. https://doi.org/10.1007/s11165-016-9602-2.

The Hill. (2019). Lawmakers introduce legislation to improve cyber workforce funding Retrieved December 21, 2019, from https://thehill.com/policy/cybersecurity/443711-lawmakers-introduce-legislation-to-improve-cyber-workforce-funding.

Treekrutpant, A. (2017). Work motivations affecting self-efficacy and work effectiveness of flight attendants of airlines in Thailand. In *2017 International Conference on Digital Arts, Media and Technology (ICDAMT)* (pp. 454–457). https://doi.org/10.1109/ICDAMT.2017.7905011.

Trevelyan, E. G., & Robinson, P. N. (2015). Delphi methodology in health research: How to do it? *European Journal of Integrative Medicine*, *7*, 423–428. https://doi.org/https://doi.org/10.1016/j.eujim.2015.07.002.

U.S. Department of Health & Human Services. Office for Civil Rights (OCR). (2010). The HIPAA security rule. Retrieved from https://www.hcca-info.org/Portals/0/PDFs/Resources/Conference_Handouts/Compliance_Institute/2016/P4handout2.pdf.

U.S. Department of Health & Human Services. (2010). Guidance on risk analysis requirements under the HIPAA security rule. Retrieved from https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html.

U.S. Department of Health & Human Services. (2015). Resolution agreements. *Health Information Privacy*. Retrieved from https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html.

U.S. Department of Health & Human Services (HHS). (2013). Business Associates.

Retrieved March 22, 2019, from https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html.

U.S. Department of Health and Human Services. (2011). *Security Standards for the Protection of Electronic Protected Health Information*. The United States.

U.S. Department of Health and Human Services (HHS). (n.d.). About HHS. Retrieved March 1, 2019, from https://www.hhs.gov/about/index.html.

U.S. Department of Health and Human Services (HHS). (2007). HIPAA Security series: #1 security 101 for covered entities, *2*, 1–11. Retrieved from http://www.cms.hhs.gov/SecurityStandard/underthe%22Regulation%22page.

U.S. Department of Health and Human Services (HHS). (2011). 45 C.F.R. § 164 Subpart C - security standards for the protection of electronic protected health information, 733–740. Retrieved from https://www.gpo.gov/fdsys/pkg/CFR-2004-title45-vol1/pdf/CFR-2004-title45-vol1-part164-subpartC.pdf

U.S. Department of Health and Human Services (HHS). (2017). The Security Rule. Retrieved March 1, 2019, from https://www.hhs.gov/hipaa/for-professionals/security/index.html.

U.S. Department of Health and Human Services (HHS). Centers for Medicare & Medicaid Services (CMMS). (2007). HIPAA security series #6: Basics of risk analysis and risk management, *2*. Retrieved from https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf.

U.S. Department of Health and Human Services (HHS). Health Insurance Reform: Security Standards, 68 45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule § (2003). https://doi.org/10.1089/hum.1996.7.15-1923.

U.S. Department of Health and Human Services (HHS). (2013). HIPAA administrative simplification regulation text. Retrieved from https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf.

U.S. Department of Health and Human Services Office for Civil Rights (OCR). (2018a). 2018 OCR HIPAA summary: Settlements and judgments, (January), 300.

U.S. Department of Health and Human Services Office for Civil Rights (OCR). (2018b). About Us (OCR). Retrieved March 1, 2019, from https://www.hhs.gov/ocr/about-us/index.html.

U.S. Department of Health and Human Services Office for Civil Rights (OCR). (2018c). *Request for Information on Modifying HIPAA Rules to Improve Coordinated Care*.

U.S. Department of Health and Human Services Office for Civil Rights (OCR). (2018d). Resolution agreements. Retrieved from https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html.

U.S. Office of Personnel Management. (n.d.). What is a subject matter expert? Retrieved from https://www.opm.gov/FAQs/QA.aspx?fid=a6da6c2e-e1cb-4841-b72d-53eb4adf1ab1&pid=c9d6d33b-a98c-45f5-ad76-497565d58bcf.

van Griethuijsen, R., van Eijck, M. W., Haste, H., den Brok, P. J., Skinner, N. C., Mansour, N., … BouJaoude, S. (2015). Global patterns in students views of science and interest in science. *Research in Science Education*, *45*(4), 581–603. https://doi.org/10.1007/s11165-014-9438-6.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management*, *49*(3–4), 190–198. https://doi.org/10.1016/J.IM.2012.04.002.

Verizon. (2019). *2019 Data Breach Investigations Report*. *Computer Fraud & Security* (Vol. 2019). https://doi.org/10.1016/s1361-3723(19)30060-0.

Vito, R. (2019). Key variations in organizational culture and leadership influence: A comparison between three children’s mental health and child welfare agencies. *Children and Youth Services Review*, *108*. https://doi.org/10.1016/j.childyouth.2019.104600.

Vogenberg, F. R. (2019). US healthcare trends and contradictions in 2019. *American Health and Drug Benefits*, *12*(1), 40–47.

Wall, J. D., Lowry, P. B., & Barlow, J. B. (2016). Organizational violations of externally governed privacy and security rules: Explaining and predicting selective violations under conditions of strain and excess. *Journal of the Association for Information Systems*, *17*(1), 39–76.

Webler, T., Levine, D., Rakel, H., & Renn, O. (1991). A novel approach to reducing uncertainty: The group Delphi. *Technological Forecasting and Social Change*, *39*, 253–263. Retrieved from http://dx.doi.org./doi:10.1016/0040-1625(91)90040-M.

Weir, I. (2018). *Spearman’s correlation*. *Statstutor*. Retrieved from http://www.statstutor.ac.uk/resources/uploaded/spearmans.pdf.

Weistroffer, H. R. (2016). Understanding deterrence theory in security compliance behavior : A quantitative meta-analysis approach. *Proceedings of the Southern Association for Information Systems Conference*, *St. Augustine, FL, USA March 18th–19th, 2016*. https://doi.org/10.1007/s12221-009-0237-z.

Wu Suen, L. J., Huang, H. M., & Lee, H. H. (2014). A comparison of convenience sampling and purposive sampling. *Journal of Nursing*, *61*(3), 105–111.

https://doi.org/10.6224/JN.61.3.105

Xiao, C., Ye, J., Esteves, R. M., & Rong, C. (2016). Using Spearman's correlation coefficients for exploratory data analysis on big datasets. *Concurrency and Computation: Practice and Experience*, *28*(14), 3866–3878. https://doi.org/10.1002/cpe.3745.

Zhang, N., & Zhang, N. (2018). Understanding the roles of challenge security demands: Psychological resources in information security policy noncompliance. *Pacis 2018*.

Zikmund, W. G., Babin, B. J., Carr, J. C., & Griffin, M. (2013). *Business research methods*. Cengage Learning.