Oct 23rd, 2:30 PM - 3:00 PM

Factors that influence HIPAA Secure compliance in small and medium-size health care facilities

Wlad Pierre-Francois
Trident, wlad.pierre-francois@my.trident.edu

Indira Guzman
Trident, Indira.Guzman@trident.edu

Abstract

This study extends the body of literature concerning security compliance by investigating the antecedents of HIPPA security compliance. A conceptual model, specifying a set of hypothesized relationships between management support, security awareness, security culture; security behavior, and risk of sanctions to address their effect on HIPAA security compliance is presented. This model was developed based on the review of the literature, Protection Motivation Theory, and General Deterrence Theory. Specifically, the aim of the study is to examine the mediating role of risk of sanctions on HIPAA security compliance.

Location

Zoom Session 1 (Main Papers Track)

Disciplines

Information Security | Management Information Systems | Technology and Innovation

INTRODUCTION

The protection of personal information, and especially electronically protected health information (ePHI), is a significant issue for healthcare organizations of all sizes. 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. The HIPAA Security Rule was created to ensure that U.S. citizens' electronic health data is protected from loss or abuse. However, previous studies have shown that small and medium healthcare facilities have difficulties with maintaining compliance with the Security Rule (2020) (Chen, 2017). An update to the HIPAA regulations of 2009 has significance to information technology and systems. In 2017, the American Recovery and Reinvestment Act title XIII created the Health Information Technology for Economic and Clinical Health Act (HITECH). It intended to create a nationwide network of electronic health records and signaled the start of the Meaningful Use Program (MUP), HIPAA Journal (2020). The updates significant addition is the (MUP). It incentivized healthcare providers to adopt technology in the provision of healthcare, HITECH had to consider both the HIPAA Privacy and Security Rules. HITECH bolsters the 1996 HIPAA by protecting the privacy and security of certain PHI (Murray, HIPAA Explained, 2020) HIPAA and HITECH Act 2009 references each other's regulations. They differ in subtle ways. Where both address the security of electronically protected health information (ePHI), their most significant difference relates to patient rights. Before HITECH, a patient could not determine who had access to their ePHI. Both Acts are equally essential, and covered entities (CE) and Business Associates (BA) are bound to comply with both Acts.

Security rule compliance is challenging to maintain by small and medium-sized health care facilities. Non-compliance research begun to examine factors that influence full Security Rule compliance. Past research has leveraged various theoretical frameworks and conceptual models to contribute to the understanding of successful HIPAA compliance by small and medium health care facilities. Martin (2015) examined a limited to non-operationalized theoretical models; Brady (2010) found that an organization's employees may be motivated to comply, but without the characteristics and capacities, compliance toward a regulatory strategy, there will still be an issue.

This literature review aims to leverage the variables of Management Support, Security Awareness, Security Culture, Security Behavior (Brady, 2010), and Risk of Sanctions (Bulgurcu, 2010) to address the effect of compliance of security rule. It looks at One, examines the impact risk of sanctions has on HIPAA compliance. Two, it discusses the impact of the factors of HIPAA and HITECH Security Rule Compliance on small and medium health facilities Information System (IS)Security

(Furstenberg, 2020). Previous studies study compliance with regulations but did not specifically address compliance with HIPPA regulations.

Research Question

The general research questions of this study are: (1) What are the antecedents of HIPPA security compliance? (2) How do Management Support, Security Awareness, Security Culture affect HIPAA Security Compliance? (3) Does Security Behavior mediate the relationship between Management Support and HIPAA Security Compliance? (4) Does the Risk of Sanctions mediate the relationship between Security Awareness, Security Culture, and HIPAA Security Compliance?

Theoretical Framework

In the effort to understand the antecedents of HIPAA Security Rule compliance, this research will propose and test a model of the factors that may be under the influence and lead to compliance. The current research will leverage several theories in this pursuit. The *theory of reasoned action (TRA)* was introduced to explain and predict human behavior. However, it was found that TRA was unable to predict behavior when users perceived they had little behavioral control. Ajzen (1991) developed the missing construct, which he named perceived behavioral control and added it to TRA, which then became known as the theory of planned behavior (TPB). According to Ajzen (1991), the perceived behavioral control component of the theory of planned behavior model is compatible with Bandura's concept of perceived self-efficacy. Self-efficacy is a construct of social cognitive theory (Bandura A. , 1998), which explains an individual's perception of their abilities to perform a given task.

The theory of planned behavior is an extension of the theory of reasoned action. The theory of planned behavior overcame the limitations of the theory of reasoned action when subjects perceived limited volitional control (Ajzen, 1991). In the theory of planned behavior (TPB), attitude, subjective norm, and perceived behavioral control were defined by Ajzen (1991) as antecedent constructs of intention. As described in TPB: attitude is a feeling towards a behavior, subjective norms are perceptions of societal expectations on subject's behavior, and perceived behavioral control are the subjects' perceptions of volitional control regarding a given intention (Ajzen, 1991) (Johnston, 2010).

The *protection motivation theory (PMT)* is a case of expectancy theory in which there is an expectancy that a consequence will follow a behavior. Protection motivation is useful in predicting how unintended risks introduced by an act of compliance can negatively impact compliance intention. Fear motivates

avoidance or escape from a noxious event and is a particularly salient predictor of behavior (Rogers, 1975, p. 95). Rogers (1975) theorized that the three components germane to a fear appeal's ability to motivate protective behavior were: the perceived severity of the event, susceptibility to the event, and the efficacy of a protective response.

The *general deterrence theory* (GDT) is grounded in criminology; it purports that swift and severe sanctions deter individuals from violating laws or rules (Gunningham, 2010). Studies based on deterrence theory (Kankanhalli, 2003) have highlighted the importance of sanctions in deterring crimes related to computer security. Sanctions are believed to lead employees to perceive that there is a cost associated with not adhering to security-related rules and regulations. Deterrence theory refers to deter criminal behavior when the expected loss (penalty of violating law) is more significant than the expected gain. It focuses primarily on the effect of penalties (Willison, 2013).

Two utilitarian philosophers of the 18th century, Cesare Beccaria and Jeremy Bentham formulated the deterrence theory to explain crime and reduce it. Beccaria and Bentham, along with other classical theorists, believed that humans are rational beings with free will to govern their own decisions. Beccaria emphasized that laws should be published so that people may know what they represent—their intent and purpose. Basing the legitimacy of criminal sanctions on the social contract, Beccaria (1963) called laws "the conditions under which men, naturally independent, united themselves in society" (p. 11). He was against torture and secret accusations and demanded they be abolished (Beccaria, 2016). Bentham's unique perspective, known as utilitarianism, is used to construct a fascinating calculus for determining which action to perform when confronted with situations requiring moral decision-making, the goal of which is to arrive at the "greatest happiness of the greatest number." Toward this end, he endeavors to delineate the sources and kinds of pleasure and pain and how they can be measured when assessing one's moral options. Bentham supports his arguments with discussions of intentionality, consciousness, motives, and dispositions. Bentham concludes this groundbreaking work with an analysis of punishment: its purpose and the proper role that law and jurisprudence should play in its determination and implementation (Bentham, 1996).

Contemporaries such as Vance, A., Siponen, M. T., & Straub, D. W. (2020) found in testing a model using deterrence theory, that informal sanctions have significant effects for those who espouse a collectivist cultural value. They also found that formal sanctions were insignificant across all cultures.

Conceptual Model

This study's conceptual model draws from several past research. Brady (2010) created and defined unique constructs that served as DVs, which defined and measured SR compliance; Martin (2015) consented in the extension and operationalization of their theoretical model. A limitation conceded was that the model framework was incomplete and suggested future researchers should expand, adapt, and use to aid in the empirical testing of HIPAA SR compliance perceptions and behaviors (Furstenberg, 2020).

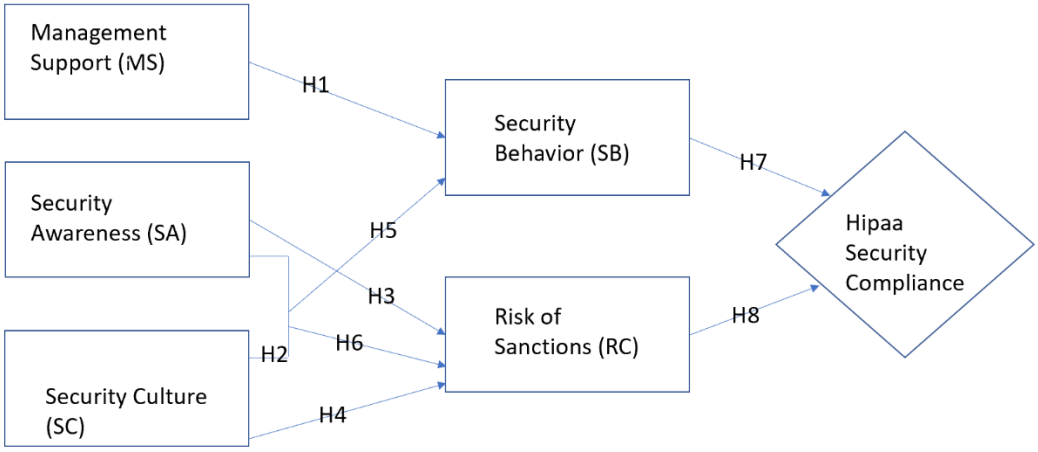


Figure 1. Conceptual Model of HIPPA Security Compliance

Research Model and Hypotheses

Most Relevant Constructs

Management support is defined as the perceived level of general support offered by top management in organizations *(Igbaria, 1997)*. Top management comprises those executives positioned in the high echelons of an organization. These executives have the legitimate power to manage organizational resources and internal workforce investments and drive strategic intentions, or the guidance provided to all levels of employees within the organization *(O'Shannassy, 2016)*. Previous studies have identified management support as one of the vital recurring factors affecting system success *(Cerveny, 1986)*. Young & Jordan *(2008)*, recognized the importance of top management support (TMS) in Information Systems (IS) literature. The success of strategic changes or management programs rests on the commitment of top management *()*. According to Young (*(2008)*, top management support (TMS) is 'when a senior management project

sponsor/champion, the CEO and other senior managers devote time to review plans, follow up on results and facilitate management problems.' The authors' found that TMS is essential in every case and provides a persuasive explanation of why the projects succeeded or failed. Young *(2008)*, concluded that TMS is not merely one of many critical success factors (CSFs) needed for project success, but is the most crucial CSF.

Security Awareness According to Bulgurcu *(2010)*, information security awareness is defined as an employee's general knowledge about information security and his cognizance of its information system policy. Siponen *(2000)* defined information security awareness as a "state where users in an organization are aware of ideally committed to their security mission (often expressed as in end-user security guidelines)." Siponen's definition can be easily extrapolated toward individual users, members of the society who might be committed not only to their interests but also to the common interest of the whole. Through this, Tsohou et al. *(2008)* noted that information security awareness is "commonly regarded as aiming at improving information security by enhancing the adoption of security policies and countermeasures, improving IS users' security behavior, and altering work routine, so that good security habits are applied." Bulgurcu *(2010)* noted that awareness of information security might be built from direct life experiences, such as having once been harmed by a virus attack or penalized for not adhering to security rules and regulations, or it can be based on information obtained from external sources, such as newspapers, professional journals, organizational policy documents, and corporate workshops. Information security awareness is an individual's knowledge of particular security threats and the potential countermeasures against those threats *(Siponen, 2000) (Thomson, 1998)*. Therefore, it is appropriate to treat information security awareness from the protective technology perspective and perceive information security as a necessity rather than a benefit.

Security culture will be examined via the lens of information security. Hellriegel, D., Slocum, J.W. Jr, and Woodman, R.W. (1988) noted that an organizational culture develops where executives and management form a vision and strategy. They posited that the vision and strategy are often depicted in corporate policies and procedures. They also believed that employee behavior would become evident, as the idea, plan, and policies will guide it. Additionally, they suggest that organizational culture will emerge to encapsulates the vision and strategy and the experienced employees had when implementing them. Corporate culture is leveraged to develop an information security culture. They found that awareness of an information security policy contributes to fostering an information security culture. The common understanding of information security culture is that it consists of a shared pattern of values, mental models, and

activities that are traded among an organization's employees over time (Karlsson, 2015). According to (Magklaras & Furnell, 2004) (Dhillon & Backhouse, 2001), the objective of developing this information security culture is to control the inappropriate use of information by the information system users. In an information security culture, the employees' behavior contributes towards the protection of data, information, and knowledge (Dhillon & Backhouse, 2001), and information security becomes a natural part of their daily activities (Schlienger & Teufel, 2003).

Security behavior was defined as behaviors to protect against security threats by adapting Protection Motivation Theory into an information security context (Crossler, 2010). According to (Ng B.-Y., 2009), it is critical to understand what will influence a user's security behavior so that appropriate awareness programs can be designed. Individual Security Behavior (ISB) exist due to many security protection mechanisms (Crossler, 2010). Vroom and Solms (2004) argue to enhance the effectiveness of security policies, and the employees must behave and act responsibly in line with the prescribed security policies of the organization. They mentioned that achieving this requires some form of investigation and evaluation of the security behavior of the individual. Tejaswini, H., Rao, H.R. (2009) found that intrinsic and extrinsic motivators can influence security behaviors. They also found that pressures exerted by subjective norms and peer behaviors influence employee information security behaviors. According to Floyd, D. L., Prentice-Dunn, S., and Rogers, R. W. (2000), Information Security (IPsec)studies have focused on security-related intentions and ignored actual behavioral change. Boss, S., Galletta, D., Lowry, P.B., Moody, G.D., Polak, P. (2015) maintain that actual behaviors are essential for ISec research because the end goal is to change security behaviors, not just security intentions. They suggest that by measuring both the intentions and actual behaviors, they can show that the path from intentions to actual behavior is more pronounced in the high fear-appeal. They stress the importance of using real fear appeals and not just security policies or global threats.

Risk of Sanctions is defined as tangible or intangible penalties such as demotions, loss of reputation, reprimands, monetary or non-monetary penalties, and negative personal mention in oral or written assessment reports incurred by an employee non-compliance with the requirements of the information systems policies (Bulgurcu, 2010). The authors suggest that sanctions are believed to lead employees to perceive that there is a cost associated with not adhering to security-related rules and regulations. According to Wenzel (2004), the rational actor approach, detection probability, and sanction severity should interact in their effects. It is their product that defines the expected value and contributes to the expected (dis)utility. The author suggests that ethics and norms are not only a

more potent means to achieve compliance with the law than deterrence is but, in fact, also delimit the relevance of deterrence. Williams and Hawkins (1986) warn that the effects of deterrence, on the one hand, and social norms, on the other hand, not be set against each other and compared with each other, as if they were independent mechanisms.

Hypotheses

No.	Hypotheses
H1	Management Support influence on Security Behavior
H2	Security Awareness influence on Security Culture
H3	Security Awareness influence on Risk of Sanction
H4	Security Culture influence on Risk of Sanction
H5	Security Awareness influence on Security Culture and Security Behavior
H6	Security Awareness influence on Security Culture and Risk of Sanctions
H7	Management Support influence on Security Awareness, Security Culture, Security Behavior result in HIPAA Security Compliance
H8	Management Support influence on Security Awareness, Security Culture, Risk of Sanctions result in HIPAA Security Compliance

METHODOLOGY

The model will be empirically tested in a correlational study. The sample and target population will be medical providers in individual to small and medium-size health care facilities in the United States. The level of analysis for this is at the individual medical practitioner level. This study is still undecided regarding the method of administering the instrument. Previous studies into HIPAA security rule compliance utilized a survey-based instrument. The leveraged survey instrument to validated and reliably test to measure various constructs (Furstenberg, 2020). Brady (2010) utilized statistical methods such as MLR and correlation analysis to test the

conceptual research model being investigated. Brady's theoretical model share factors with this study in looking for impacts on HIPAA security rule compliance in small-medium-sized health facilities. Future partners to access the subjects for this study should include national, state, and specialty professional advocacy

groups. As the study does not address patient information, HIPAA security concerns should not pose problems for the instrument's distribution.

Measures

The data will be analyzed using SPSS for Windows. The IVs, DV, and all survey questions will be summarized using the mean, standard deviation, and range for continuous scaled variables, and frequency and percent for categorical scaled variables (Tabachnick, 2019). The study will establish the instruments internal consistency reliability using Cronbach's alpha statistical analysis (Tabachnick, 2019). Cronbach's alpha will be used to measure the internal consistency reliability of the IV scale scores of Management Support (MS), Security Awareness (SA), Security Culture (SC), Security Behavior (SB), Risk of Sanction (RS), and HIPAA Security Compliance. The Cronbach's alpha statistic will be used to evaluate internal consistency reliability, with the ordinary rule-of-thumb being, a Cronbach's alpha of 0.70 or higher indicates acceptable reliability (Tabachnick, 2019). The constructs of this study were built on existing constructs within the literature. They were adapted from existing survey questions and sought to emphasize possible associations and interactions between factors enforcing or encouraging the perceived likelihood of security rule compliance in Covered Entities & Business Associates (Parker, 2017).

Table 1 – Constructs of this study

Construct	Type	Source	Items
Management Support (M-S)	Reflective	James William Brady. 2010.	10
Security Awareness (S-A)	Reflective	James William Brady. 2010.	10
Security Culture (S-C)	Reflective	James William Brady. 2010.	10
Security Behavior (S-B)	Reflective	James William Brady. 2010.	9
Risk of Sanction (R-S)	Reflective	Bulgurcu et al. (2010).	4
HIPAA Security Compliance	Reflective	Bulgurcu et al. (2010).	8

Table 2 – Survey questions

Demographic Questions	
Age	Please enter your age in years
Highest education level completed	Less than HS, HS, undergraduate, Masters, advanced degree.
Area of work in your company	IT, Sales, Marketing, Accounting, HR, Other
Source and Scale Reliability for Management Support	
Management Support: Variable definition "The degree that senior management understands the importance of the security function and the extent to which management is perceived supporting security goals and priorities" (Knapp, 2006). Adaptation Source: James William Brady. 2010. An Investigation of Factors that Affect HIPAA Security Compliance in Academic Medical Centers. Doctoral dissertation. Nova Southeastern University. Retrieved from NSUWorks, Graduate School of Computer and Information Sciences. (100) https://nsuworks.nova.edu/gscis_etd/100. The following is a list of statements related to the influence of management support on HIPAA security compliance at your organization. Please read each item and rate the level of agreement you attribute to each statement from: (1) 'Strongly Disagree' to (5) 'Strongly Agree'.	
Original Question	**Adapted Question**
Top management considers HIPAA security compliance an important organizational priority in my organization.	Top management considers HIPAA security compliance an important organizational priority in my organization.
Top executives are interested in HIPAA security compliance issues in my organization.	Top executives are interested in HIPAA security compliance issues in my organization.
Top management takes HIPAA security compliance issues into account when planning corporate strategies in my organization.	Top management takes HIPAA security compliance issues into account when planning corporate strategies in my organization.
Senior leadership's words and actions demonstrate that HIPAA security compliance is a priority in my organization.	Senior leadership's words and actions demonstrate that HIPAA security compliance is a priority in my organization.

Visible support for HIPAA security compliance goals by senior management is obvious in my organization.	Visible support for HIPAA security compliance goals by senior management is obvious in my organization.
Senior management gives strong and consistent support to my organization's HIPAA security compliance program in my organization.	Senior management gives strong and consistent support to my organization's HIPAA security compliance program in my organization.
Top managers think that HIPAA security compliance is beneficial in my organization.	Top managers think that HIPAA security compliance is beneficial in my organization.
Top managers always support and encourage employees complying with HIPAA security requirements in my organization.	Top managers always support and encourage employees complying with HIPAA security requirements in my organization.
Top managers provide most of the necessary help and resources to enable employees to comply with HIPAA security requirements in my organization.	Top managers provide most of the necessary help and resources to enable employees to comply with HIPAA security requirements in my organization.
Top managers are keen to see that the employees are happy to comply with HIPAA security requirements in my organization.	Top managers are keen to see that the employees are happy to comply with HIPAA security requirements in my organization.

Source and Scale Reliability for Security Awareness
Security Awareness: Variable definition: is a "state where users in an organization are aware of ideally committed to their security mission (often expressed as in end-user security guidelines)." Siponen (2000). Definition for this Study: "commonly regarded as aiming at improving information security by enhancing the adoption of security policies and countermeasures, improving IS users' security behavior, and altering work routine so that good security habits are applied" Tsohou (2008). Adaptation Source: James William Brady. 2010. An Investigation of Factors that Affect HIPAA Security Compliance in Academic Medical Centers. Doctoral dissertation. Nova Southeastern University. Retrieved from NSUWorks, Graduate School of Computer and Information Sciences. (100) https://nsuworks.nova.edu/gscis_etd/100.

The following is a list of statements related to the influence of security awareness on HIPAA security compliance at your organization. Please read each item and rate the level of agreement you attribute to each statement from: (1) Strongly Disagree' to (5) 'Strongly Agree'. Items Strongly Disagree, Disagree Neither Disagree nor Agree Agree Strongly Agree 1 2 3 4 5	
Original Question	**Adapted Question**
My organization provides HIPAA security awareness training to help employees improve their awareness of computer and information security issues.	My organization provides HIPAA security awareness training to help employees improve their awareness of computer and information security issues.
In my organization, employees are briefed on the consequences of modifying computerized data in an unauthorized way.	In my organization, employees are briefed on the consequences of modifying computerized data in an unauthorized way.
My organization educates employees on their computer security responsibilities.	My organization educates employees on their computer security responsibilities.
In my organization, employees are briefed on the consequences of accessing computer systems that they are not authorized to use.	In my organization, employees are briefed on the consequences of accessing computer systems that they are not authorized to use.
An effective HIPAA security awareness program exists at my organization.	An effective HIPAA security awareness program exists at my organization.
A continuous, ongoing HIPAA security awareness program exists at my organization.	A continuous, ongoing HIPAA security awareness program exists at my organization.
Users receive adequate HIPAA security awareness refresher training appropriate for their job function at my organization.	Users receive adequate HIPAA security awareness refresher training appropriate for their job function at my organization.
HIPAA security awareness is an ongoing focus at my organization	HIPAA security awareness is an ongoing focus at my organization
HIPAA security awareness training is of sufficient length at my organization.	HIPAA security awareness training is of sufficient length at my organization.
HIPAA security awareness training at my organizations helps me see the usefulness of following certain procedures to safeguard patient	HIPAA security awareness training at my organizations helps me see the usefulness of following certain procedures to safeguard patient

privacy.	privacy.

Source and Scale Reliability for Security Culture

Security Culture:
Variable definition by Volonino, L., & Robinson, S. R. (2004): "A focus on security in the development of information systems and networks and the adoption of new ways of thinking and behaving when using and interacting within information systems and networks"

Adaptation Source: James William Brady. 2010. An Investigation of Factors that Affect HIPAA Security Compliance in Academic Medical Centers. Doctoral dissertation. Nova Southeastern University. Retrieved from NSUWorks, Graduate School of Computer and Information Sciences. (100) https://nsuworks.nova.edu/gscis_etd/100.

The following is a list of statements related to the influence of security culture on HIPAA security compliance at your organization. Please read each item and rate the level of agreement you attribute to each statement from: (1) 'Strongly Disagree' to (5) 'Strongly Agree'.

Original Question	**Adapted Question**
Employees at my organization value the importance of security.	Employees at my organization value the importance of security.
A culture exists at my organization that promotes good security practices.	A culture exists at my organization that promotes good security practices.
Security has traditionally been considered an important organizational value at my organization.	Security has traditionally been considered an important organizational value at my organization.
Practicing good security is the accepted way of doing business at my organization.	Practicing good security is the accepted way of doing business at my organization.
The overall environment at my organization fosters security-minded thinking.	The overall environment at my organization fosters security-minded thinking.
Information security at my organization is a key norm shared by my fellow employees.	Information security at my organization is a key norm shared by my fellow employees.
My organization sets high standards for the protection of its information assets.	My organization sets high standards for the protection of its information assets.
Management at my organization is	Management at my organization is

concerned with information security.	concerned with information security.
My immediate supervisor is concerned with information security for the organization.	My immediate supervisor is concerned with information security for the organization.
My coworkers are concerned with information security for the organization.	My coworkers are concerned with information security for the organization.
Source and Scale Reliability for Security Behavior	
Security Behavior: Variable definition by Chan, M., Woon, I., & Kankanhalli, A. (2005): "the set of core information security activities that need to be carried out by individuals to maintain information security as defined by information security policies" Adaptation Source: James William Brady. 2010. An Investigation of Factors that Affect HIPAA Security Compliance in Academic Medical Centers. Doctoral dissertation. Nova Southeastern University. Retrieved from NSUWorks, Graduate School of Computer and Information Sciences. (100) https://nsuworks.nova.edu/gscis_etd/100. The following is a list of statements related to the influence of secure behavior on HIPAA security compliance at your organization. Please read each item and rate the level of agreement you attribute to each statement from: (1) 'Strongly Disagree' to (5) 'Strongly Agree'.	
Original Question	**Adapted Question**
I will comply with HIPAA security procedures at my organization when performing my daily work.	I will comply with HIPAA security procedures at my organization when performing my daily work.
I tend to ignore HIPAA security procedures at my organization that I think are not necessary (reverse).	I tend to ignore HIPAA security procedures at my organization that I think are not necessary (reverse).
I tend to ignore HIPAA security procedures at my organization in order to complete my work quickly (reverse).	I tend to ignore HIPAA security procedures at my organization in order to complete my work quickly (reverse).
Sometimes I comply with HIPAA security procedures at my organization when it affects the performance/productivity of my work (reverse).	Sometimes I comply with HIPAA security procedures at my organization when it affects the performance/productivity of my work (reverse).

I tend to comply with HIPAA security procedures at my organization only when it is convenient to do so (reverse).	I tend to comply with HIPAA security procedures at my organization only when it is convenient to do so (reverse).
Exhibiting good security behavior is rewarded at my organization.	Exhibiting good security behavior is rewarded at my organization.
I intend to continue complying with HIPAA security requirements at my organization.	I intend to continue complying with HIPAA security requirements at my organization.
I predict I will comply with HIPAA security requirements at my organization.	I predict I will comply with HIPAA security requirements at my organization.
I plan to continue to safeguard patient and security at my organization.	I plan to continue to safeguard patient and security at my organization.

Source and Scale Reliability for Risk of Sanctions

Risk of Sanctions:
Variable definition by Khazaei, Amir & Manjiri, Hadi & Samiey, Ebrahim & Najafi, Hossein, 2014: a judgment made by consumers according to their sense of control over the management, utilization, and conversion of their time and effort in achieving their goals associated with access to and use of the service. Reliability alpha was .785.

Definition for this study:
Adaptation Source: Bulgurcu, Burcu; Cavusoglu, Hasan; and Benbasat, Izak. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," MIS Quarterly, (34: 3) pp.523-548.

Question to participants: 1 = Not at All;2 = Very Rarely; 3 = Rarely; 4 = Occasionally; 5 = Frequently; 6 = Very Frequently; 7 = Very Much scale.

Original Question	**Adapted Question**
I will probably be punished or demoted if I do not comply with the requirements of the ISP. _____	I will probably be punished or demoted if I do not comply with the requirements of the security rule enforcement of self-reporting.
I will receive personal reprimand in oral or written assessment reports if I do not comply with the requirements of the ISP.	I will probably be punished or demoted if I do not comply with the requirements of the security rule enforcement of self-reporting.
I will incur monetary or non-monetary	I will incur monetary or non-monetary

penalties if I do not comply with the requirements of the ISP.	penalties if I do not comply with the requirements of the security rule enforcement of self-reporting.
My facing tangible or intangible sanctions is tied to whether I do not comply with the requirements of the ISP.	My facing tangible or intangible sanctions is tied to whether I do not comply with the requirements of the security rule enforcement of self-reporting.
Source and Scale Reliability for HIPAA Security Compliance	
HIPAA Security Compliance: Variable definition by Mayer, Ehrhart & Schneider, 2009: Customer satisfaction with the people working in the departments. Reliability alpha was .94. Adaptation Source: Bulgurcu, Burcu; Cavusoglu, Hasan; and Benbasat, Izak. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," MIS Quarterly, (34: 3) pp.523-548. Question to participants: 1 = Not at All;2 = Very Rarely; 3 = Rarely; 4 = Occasionally; 5 = Frequently; 6 = Very Frequently; 7 = Very Much scale.	
Original Question	**Adapted Question**
HIPAA Security Rule (non) Compliance Behaviors (Perceived Cost of Noncompliance)	
My noncompliance with the requirements of the ISP would be harmful to me	My noncompliance with the requirements of the HIPAA security rules would be harmful to me
My noncompliance with the requirements of the ISP would impact me negatively	My noncompliance with the requirements of the ISP would impact me negatively
My noncompliance with the requirements of the ISP would create disadvantages for me	My noncompliance with the requirements of the HIPAA security rules would create disadvantages for me
My noncompliance with the requirements of the ISP would generate losses for me	My noncompliance with the requirements of the HIPAA security rules would generate losses for me
HIPAA Security Rule Compliance Behaviors (Perceived Benefit of	

Compliance)	
Original Question	**Adapted Question**
My compliance with the requirements of the ISP would be favorable to me	My compliance with the requirements of the HIPAA security rules would be favorable to me
My compliance with the requirements of the ISP would result in benefits to me	My compliance with the requirements of the HIPAA security rules would result in benefits to me
My compliance with the requirements of the ISP would create advantages for me	My compliance with the requirements of the HIPAA security rules would create advantages for me
My compliance with the requirements of the ISP would provide gains to me	My compliance with the requirements of the HIPAA security rules would provide gains to me
Opinions / open ended questions	
What is your biggest complaint when dealing with HIPAA security rules	
Do you think HIPAA security rules work?	
Do you think HIPAA security rules work are effective in your organization?	

Future Research

In later research, a dive into recidivist rates of sanctioned could be explored. A comparison can be made between sanctioned individuals of facilities and the facilities (management) being sanctioned. A cause and effect analysis may determine the impact individuals or management have on the rate of repeat offenders.

CONCLUSIONS AND LIMITATIONS

This research study will be limited to factors affecting HIPAA Security Rule compliance in small and medium-size health care facilities within the U.S. Senior management of these facilities will benefit from this study, as well as HIPAA compliance researchers. The target participants of this research will be senior management, members of I.T., and medical staff of small and medium-size health care facilities. Consequently, there are no apparent adverse risks to this study. The study aims to contribute to the understanding of factors that affect HIPAA security rule compliance. It contributes to the literature in several areas, including regulatory compliance, management support, security awareness, security behavior, security culture, risk of sanctions, and healthcare policy.

REFERENCES

Ajzen, I. (1991). The theory of planned behavior. Organizational Behavior and Human Decision Processes, 50(2), 179-211. doi:10.1016/0749-5978(91)90020-T

Bandura, A. &. (1989). Effect of perceived controllability and performance standards on self-regulation of complex decision making. Journal of Personality and Social Psychology, 56, 805-814.

Bandura, A. (1998). Organizational applications of social cognitive theory. Australian Journal of Management, 275-302.

Beccaria, C. (2016). On crimes and punishments. Transaction Publishers.

Bentham, J. (1996). The collected works of Jeremy Bentham: An introduction to the principles of morals and legislation. Clarendon Press.

Boss, S. G. (2015). What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors. MIS Quarterly, 39(4), 837–864.

Brady, J. (2010). An Investigation of Factors that Affect HIPAA Security Compliance in Academic Medical Centers. NSUWorks, Graduate School of Computer and Information Sciences, 1-219. Retrieved from https://nsuworks.nova.edu/gscis_etd/100.

Bulgurcu, B. C. (2010). Information Security Policy Compliance: An Emperical Study of Rationality-Based Beliefs and Information Security Awareness. MIS Quarterly, 34(3), 523-548.

Cerveny, R. a. (1986). Implementation and Structural Variables. Information & Management, 11, 192-198.

Chan, M. W. (2005). Perceptions of information security in the workplace: Linking information security climate to compliant behavior. Journal of Information Privacy & Security, 1(3), 18-41.

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

Crossler, R. E. (2010). Protection Motivation Theory: Understanding Determinants to Backing Up Personal Data. 43rd Hawaii International Conference on System Sciences (pp. 1-10). Honolulu: IEEE.

Dhillon, G., & Backhouse, J. (2001). Current directions in information systems security research: Toward socio-organizational perspectives. Information Systems Journal, 127-153.

Floyd, D. L.-D. (2000). A Meta-Analysis of Research on Protection Motivation Theory. Journal of Applied Social Psychology, 30(2), 407-429.

Furstenberg, J. J. (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. Retrieved from https://nsuworks.nova.edu/gscis_etd/1107/

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

Hellriegel, D. S. (1988). Organizational behavior, 8th edn. South-Western College Publishing.

HHS.gov. (2019, November 19). Summary of the HIPAA Security Rule. Retrieved from HHS.gov: https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

Igbaria, M. C. (1997). Personal Computing Acceptance Factors in Small Firms: A Structural Equation Model. MIS Quarterly, 279-305.

Johnston, A. C. (2010). Fear appeals and information security behaviors: An empirical study. MIS Quarterly, 549-566. Retrieved from Retrieved from http://www.tourolib.org/

Journal, H. (2017). HIPAA Explained. HIPAA Journal. Retrieved from https://www.hipaajournal.com/hipaa-explained/

Journal, H. (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/

Kankanhalli, A. T.-H.-K. (2003). An Integrative Study of Information Systems Security Effectiveness. International Journal of Information Management, 23(2), 139-154.

Karlsson, F. A. (2015). Information security culture – State-of-the-art review between 2000 and 2013. Information and Computer Security, 23(3), 246-285. Retrieved from https://search-proquest-com.ezproxy.trident.edu/docview/2093336475/fulltext/618AB854D2A7478DPQ/1?accountid=28844

Ma, Q. J. (2008). Information security management objectives and practices: A parsimonious framework. Information Management & Computer Security, 16(3), 251-270.

Magklaras, G., & Furnell, S. (2004). The insider misuse threat survey: Investigating IT misuse from legitimate users. Information Warfare & Security Conference, (pp. 42-51). Perth.

Martin, N. I. (2015). HIPAA Security Rule Compliance in small Healthcare Facilities: A Theoretical Framework. Information Systems, 16(1), 180-188.

Murray, P. (2020). HIPAA Explained. HIPAA Journal. Retrieved from https://www.hipaajournal.com/hipaa-explained/

Murray, P. (2020, May). OCR HIPAA enforcement: Summary of 2016 HIPAA settlements. HIPAA Journal. Retrieved from www.hhs.gov: https://www.hipaajournal.com/ocrhipaa-enforcement-summary-2016-hipaa-settlements-8646/

Ng B.-Y., K. A. (2009). Studying users' computer security behavior: A health belief perspective. Decision Support Systems, 46(4), 815-825.

Niehoff, B. P. (1990). The impact of top-management actions on employee attitudes and perceptions. Group and Organization Studies, 15(3), 337-352.

O'Shannassy, T. F. (2016). Strategic intent: The literature, the construct and its role in predicting organization performance. Journal of Management & Organization, 22(5), 583-598.

Parker, C. &. (2017). Regulatory Theory: Foundations and applications. Acton ACT: ANU Press. Retrieved from www.jstor.org/stable/j.ctt1q1crtm.21

Rodgers, R. H. (1993). Influence of top management commitment on management program success. Journal of Applied Psychology, 78(1), 151-155.

Rodgers, R. H. (1993). Influence of top management commitment on management program success. Journal of Applied Psychology, 78(1), 151-155.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. Journal of Psychology, 91, 93-114.

Schlienger, T., & Teufel, S. (2003). Information security culture—From analysis to change. In Proceedings of the 3rd Annual IS South Africa Conference, (pp. 9-11). Johannesburg.

Siponen, M. (2000). A conceptual foundation for organizational information security awareness. Information Management & Computer Security, 8(1), 31-41. doi:10.1108/09685220010371394

Siponen, M. (2000). A conceptual foundation for organizational information security awareness. Information Management & Computer Security, 8(1), 31-41. doi:10.1108/09685220010371394

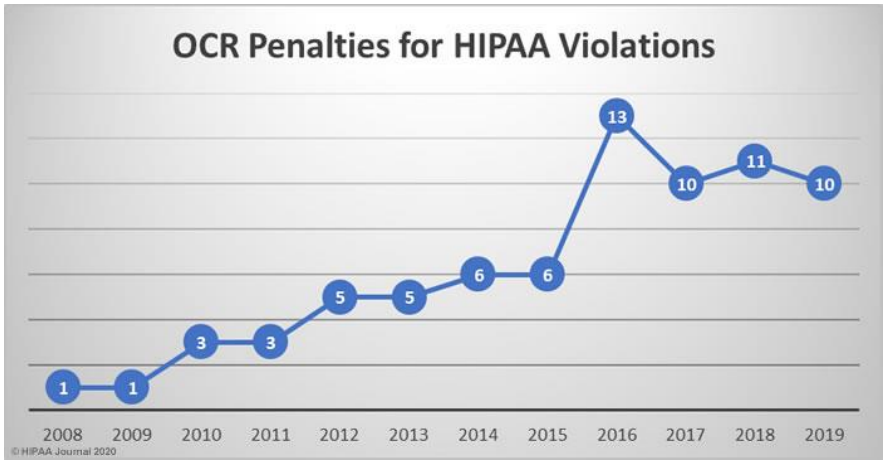
Tabachnick, B. G. (2019). Using multivariate statistics (Vol. 7). Boston: Pearson.

Tejaswini, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems, 47(2), 154-165.

Thomson, M. E. (1998). Information security awareness: Educating your users effectively. Information Management & Computer Security, 6(4), 167-173. doi:10.1108/09685229810227649
Tsohou, A. K. (2008). Process-variance models in information security awareness research. Information Management & Computer Security, 16(3), 271-287.
Tsohou, A. K. (2008). Process-variance models in information security awareness research. Information Management & Computer Security, 16(3), 271-287.
Vance, A. S. (2020). Effects of sanctions, moral beliefs, and neutralization on information security policy violations across cultures. Information & Management, 57(4), 103-212. Retrieved from https://doi.org/10.1016/j.im.2019.103212
Volonino, L. &. (2004). Principles and practice of information security: Protecting computers from hackers and lawyers. Upper Saddle River: Pearson Prentice Hall.
Vroom, C. &. (2004). Towards information security behavioural compliance. Computers & Security, 23(3), 154-165.
Wenzel, M. (2004). The Social Side of Sanctions: Personal and Social Norms as Moderators of Deterrence. Law and Human Behavior, 28(5), 547-567. Retrieved from 10.1023/B:LAHU.0000046433.57588.71
Williams, K. R. (1986). Perceptual research on general deterrence: A critical review. Law and Society Review, 545-572.
Willison, R. a. (2013). Beyond Deterrence: An Expanded View of Employee Computer Abuse. MIS Quarterly, 37(1), 1-20.
Young, R. &. (2008). Top management support: Mantra or necessity? International Journal of Project Management, 26(7), 713-725. Retrieved from https://doi.org/10.1016/j.ijproman.2008.06.001

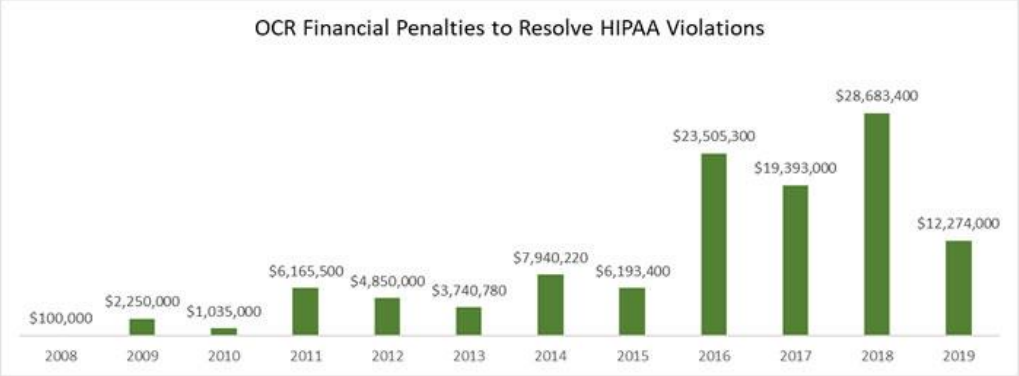
APPENDIX A: GRAPHS AND TABLES

Financial Penalties Imposed on Covered Entities and Business Associates by the HHS' Office for Civil Rights (Journal, HIPAA Explained, 2017)



Penalties for HIPAA Violations 2008-2019

(Murray, HIPAA Explained, 2020)



HIPAA Violation Cases

(Murray, HIPAA Explained, 2020)

Year	Violator	Violation	Cost
2019	West Georgia Ambulance	failure to implement HIPAA Security Rule policies and procedures	$65,000
	Bayfront Health St. Petersburg	HIPAA Right of Access failure	$85,000
	Korunda Medical, LLC	HIPAA Right of Access failure	$85,000
	University of Rochester Medical Center	risk analysis failures and risk management failure	$3 million
	Sentara Hospitals	impermissible disclosure of PHI	$2.175 million
	Elite Dental Associates	impermissible disclosures of PHI	$10,000

	Medical Informatics Engineering	risk analysis failure	$100,000, $900,000
2018	Touchstone Medical Imaging	risk analysis failure, a failure to respond to a security incident, a breach notification failure, media notification failure	$3 million
	Texas Department of Aging and Disability Services	risk analysis failure, access control failure, information system activity monitoring failure, and an impermissible disclosure	$1.6 million
	Jackson Health System	HIPAA Privacy Rule, Security Rule, and Breach Notification Rule	$2.154 million
	Cottage Health	risk analysis failures, risk management failures, a failure to conduct technical and non-technical evaluations	$ 3 million
	Pagosa Springs Medical Center	failed to enter into a BAA with a business associate	$111,400