Issues in Information Systems
Volume 16, Issue I, pp. 180-188, 2015

HIPAA SECURITY RULE COMPLIANCE IN SMALL HEALTHCARE FACILITIES: A THEORETICAL FRAMEWORK

Nancy L. Martin, Southern Illinois University Carbondale, nlmartin@siu.edu
Thomas Imboden, Southern Illinois University Carbondale, timboden@siu.edu
David T. Green, Governors State University, dgreen@govst.edu

ABSTRACT

The protection of personal information is an area of growing concern for individuals, organizations, and governments. Threats to information security in the healthcare sector carry additional risk since not only are patients' identities and financial information at risk, but health data is at risk as well. The exposure of sensitive information can cause financial hardship, mental anguish, and in healthcare, lead to social stigma and impacts on medical decisions and treatment [3]. Health information is protected through federal regulation yet many healthcare facilities struggle to meet those requirements due to a variety of factors. This paper presents a theoretical framework of potential drivers of (non)compliance behaviors that may increase understanding of the barriers that small facilities face. The framework and propositions are presented.

Keywords: Information Security, Healthcare, HIPAA Security Rule, Compliance Theory

INTRODUCTION

The protection of personal information stored electronically is an area of growing concern for individuals, organizations, and governments; and nearly all industries and organizations are vulnerable to information security threats. Threats to information security in the healthcare sector carry additional risk since not only are patients' identities and financial information at risk, but health data is at risk as well. The exposure of sensitive information can cause financial hardship, mental anguish, and especially in healthcare, lead to social stigma and impacts on medical decisions and treatment [3]. A recent report analyzed incidents of health related data breaches, and since 2009, 804 large breaches (more than 500 individuals impacted) have affected more than 29.2 million patients [34]. It is clear that in the healthcare setting, information security is of paramount importance. While academic research on issues surrounding information security in healthcare is growing, it is still an undeveloped stream and in need of further attention [3].

The privacy and security of patient information has long been a priority of medical practitioners and consumers [e.g., 35]. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) enacted broad federal regulations specifically for protected health information (PHI) [18]. HIPAA protections apply to covered entities (CE) which include healthcare providers, health plans, healthcare clearinghouses, and all their respective business associates. The HIPAA statute consists of five sections, one of which addresses information privacy and security. That HIPAA section was implemented as two administrative rules: HIPAA Privacy Rule [21] and HIPAA Security Rule [22]. The Privacy Rule focuses on policies and procedures that give individuals greater rights and privacy protections for health information and applies to all formats of PHI: electronic, paper, and oral. The HIPAA Security Rule protects electronic health information specifically and applies to entities that create, maintain, or transmit PHI. The Security Rule requires that entities ensure the confidentiality, integrity, and availability of electronic PHI, protect PHI against reasonably anticipated threats and inappropriate use or disclosure, and ensure employee compliance with the regulation requirements.

The Health Information Technology for Economic and Clinical Health (HITECH) Act was passed as part of the American Reinvestment and Recovery Act of 2009 [1] and made significant changes to HIPAA to better safeguard patient PHI and enforce Security Rule requirements. The final HITECH rule, implemented in 2013, expanded the definition of covered entities which must adhere to HIPAA requirements and increased penalties for noncompliance [17]. Among other changes, HITECH also expanded patients' rights related to access and use of PHI and breach notification.

With the worldwide attention on data breaches and, in the U.S., the federal, and sometimes additional state, mandates to secure PHI, one might assume that all healthcare facilities dutifully comply with the HIPAA Security Rule requirements to safeguard PHI. However, although HIPPA compliance research is scarce, most of what exists is focused on hospitals or other large facilities and the factors that can affect their compliance. Interestingly, these studies report variable levels of compliance [2, 4, 14]. If hospitals and other large facilities are not fully Security Rule compliant, it seems logical to conclude that small facilities face similar and possibly additional constraining factors.

Small organizations across all industries face difficulties inherent to size including limited financial, expertise, and staffing capabilities. Regarding information security, small organizations may have limited understanding of technologies and controls [10, 15], and have been found to be less likely to implement security policies and other preventative measures [24]. In a small healthcare facility, many times a solo or few physicians, or perhaps an office manager, are all the "top management" and information technology (IT) experts that exist. For this reason, small facilities likely face hardships in their efforts to comply with all facets of the Security Rule. There is scant research that addresses barriers to compliance in small facilities which may include physician, chiropractic, or dental practices, physical therapy offices, labs, nursing homes, and others types of service providers. When considering that in the U.S., more than 60 percent of physicians practice in what can be considered a small business [23], the need for more attention to information security in small healthcare facilities becomes clear. Not only is this population at risk as a small enterprise, but facilities and individuals may also be subject to civil and criminal penalties in the event of a PHI breach.

The purpose of this study is to build upon the previous exploratory work of other researchers [27] by developing a theoretical model of information security compliance behavior in small healthcare facilities. Through the lens of compliance theory, the authors discovered a number of factors that may help explain the (non)compliance behaviors of small healthcare facilities in the U.S. This paper proceeds by reviewing the HIPAA Security Rule and regulatory compliance theory, introducing a theoretical framework with propositions identifying potential drivers of (non)compliance behavior in small healthcare facilities, and discussing the implications of this research.

LITERATURE REVIEW

HIPAA Security Rule

The HIPAA Security Rule requires that CEs perform a risk analysis, implement reasonable and appropriate security measures, and document and maintain policies and procedures. These requirements are further delineated through numerous administrative, technical, physical, and organizational standards, many with implementation specifications. The technical and physical standards address security concerns such as facility access, workstation security, data integrity, user authentication, and data transmission. Administrative safeguards require processes and procedures for information access management, security awareness and training, incident procedures, and security management processes.

The Security Rule is enforced by the Office of Civil Rights (OCR) within the U.S. Department of Health and Human Services (HHS). Enforcement is usually accomplished through the investigation of complaints filed with OCR, but OCR also conducts a limited number of random compliance audits of CEs. Additionally, OCR may investigate as a result of a breach notification. The HIPAA Breach Notification Rule [20] requires CEs and their business associates to notify affected individuals and the Secretary of HHS of PHI breaches within 60 days of the breach discovery. Breaches affecting more than 500 individuals must also be reported to prominent media outlets in the affected geographic area.

Once a violation is established, OCR classifies it into one of four levels, depending on the knowledge and intent of the responsible party. Civil penalties can range from $100 to $50,000 per violation up to an annual maximum of $1.5 million. Criminal penalties for "knowingly" obtaining or disclosing PHI include up to $50,000 in fines and one year in prison. If the offenses are committed with the intent to sell, transfer, or use PHI for commercial advantage, personal gain or malicious harm, fines rise to potentially $250,000 and prison terms to 10 years. Most investigations are resolved through voluntary compliance, corrective actions, or resolution agreement among the parties. OCR may choose to impose civil penalties if the CE does not resolve the violation issue satisfactorily. Criminal violations are

referred to the Department of Justice for investigation [43]. With risk of financial and civil penalties and negative public response to data breaches, it is reasonable to assume that all healthcare facilities would prefer to be in full Security Rule compliance.

Regulatory Compliance Theory

Regulatory compliance and noncompliance are complex concepts that have drawn the interest of scholars for decades. The law and economics literatures, in particular, contribute a great deal of research dedicated to understanding the numerous, and often conflicting, motivations that lead to (non)compliance behaviors in organizations. Compliance is understood as behavior fitting expectations communicated to regulatees [8, 12]. Regulatory compliance may result due to the pursuit of goals such as maximizing utility, fulfilling a moral obligation such as duty or trust, or avoiding sanctions [5]. Noncompliance behaviors are sometimes explained as miscommunication of policy expectations or the regulatees' inability to comprehend or understand regulatory instructions [5]. Etienne [12] sought to coherently synthesize much of this work while addressing some notable missing links.

Within regard to HIPAA compliance, most studies have focused on overall HIPAA compliance rather than on Security Rule compliance [e.g. 2, 44]. Security Rule compliance has been addressed in only a limited number of studies and with few attempts to explain regulatee behavior. In one study, professionals associated with academic medical centers were surveyed to identify factors that affect Security Rule compliance [4]. In the study, the author found that user awareness of security, the security culture of the organization, and management support for information security were factors that indirectly affected Security Rule compliance [4]. In another study of healthcare organizations, researchers found that many facilities did not have the proper mechanisms in place to protect PHI as required by the Security Rule, but the study did not identify barriers to the implementation of such mechanisms [14]. Security awareness in healthcare organizations was examined by others, but did not establish compliance status or identify potential barriers to compliance [29]. Based on the limited attention paid to Security Rule compliance, especially in small facilities, it becomes evident that it is an area in need of further scrutiny.

Regulatory compliance theory is a fitting lens through which to explore the behaviors tied to HIPAA Security Rule compliance because it may offer appropriate explanations for a variety of (non)compliance behaviors. For example, many scholars have recognized that differences in resources, technical skills, and managerial oversight explain the varying levels of regulatory compliance in organizations [e.g. 32, 45]. Others have identified factors such as changes in social norms and public expectations of organizations as effecting compliance behaviors [e.g. 11, 39]. The categories and specific factors in the framework presented in this paper are based on compliance theory and previous studies in an attempt to explain Security Rule (non)compliance.

EXPLAINING SECURITY RULE COMPLIANCE/NONCOMPLIANCE BEHAVIOR

In this section, we develop a theoretical framework and propositions to explain Security Rule (non)compliance in small healthcare facilities. The framework is based upon prior research and describes four categories of drivers of Security Rule (non)compliance behavior: resource capacities, enforcement environment, social and normative pressures, and organizational factors. We posit that variation in Security Rule compliance among small healthcare facilities can be understood by examining factors in each of these categories. The graphic form of the framework is presented in the Appendix.

Resource Capacities. It is well established that regulated organizations vary in relation to a variety of resources such as knowledge about the law and regulations, technical skills, and managerial capacity and oversight, and that these differences largely explain differences in compliance behavior [e.g., 31, 32, 45]. With regard to Security Rule compliance, the capacity to acquire certain resources may likely impact to a facility's ability to fully comply.

Knowledge/understanding of requirements. As an important precursor to compliance, organizations must be aware of, and understand the need for, PHI security and the specific requirements of the Security Rule. It is unlikely that a healthcare facility would not be aware of the Security Rule requirements in general. However, staff may not have knowledge or understanding of the specific guidelines. More importantly, they may not grasp what the rule requires them to do, how to implement, or how to evaluate and monitor the steps taken to address the requirements.

There could be a lack of understanding of both the legislation and of basic information security principles which has been common in other industries [46].

P1: The level of understanding of the Security Rule requirements will affect compliance behavior.

Awareness of threats. User awareness of existing and potential security threats is a critical precursor to proper security behavior which in turn impacts information security effectiveness in organizations [e.g., 4, 16, 26]. Therefore, awareness of existing and potential security threats is also crucial to Security Rule compliance. However, facilities may not be aware of PHI security problems within their organization. For example, some small medical practices reported that they were unsure if their practice had suffered an information security incident in the past [27]. Lack of awareness, or ignorance of an existing problem, or potential problems, with PHI security could arise from an inadequate knowledge of requirements and principles, but also from over-familiarity with current PHI handling leading to noncompliance being overlooked.

P2: The level of awareness of existing and potential PHI security threats will affect compliance behavior.

Access to relevant information. There is an abundance of information about the Security Rule and its implementation throughout the HHS website, the US Department of Commerce National Institute for Standards and Technology website, and from professional organizations (e.g., American Medical Association; Health Information Management Systems Society). In fact, there is so much available information that it may lead to overload or confusion about where to obtain only the necessary information to meet the PHI security requirements. Researchers have found that often there is a problem with overprovision of information resulting in confusion about the relevance to achieving regulatory compliance [46]. Others report that information overload and lack of awareness of where to get information about regulations affect organizations' ability to comply with regulations [38].

P3: The amount of available information about Security Rule implementation will affect compliance behavior.

Access to expertise. General IT competence has been shown to be important in the effective implementation of information security [7]. IT competence might include the generation, updating, and use of security policies, or having the means to monitor unauthorized or suspicious access to PHI. If these competencies exist, it is reasonable that overall Security Rule compliance is more likely to occur. However, small healthcare facilities are less likely to have dedicated IT personnel which adds to the difficulty of obtaining the necessary expertise to meet the Security Rule requirements. Still, HIPAA requires each facility to specifically identify who is ultimately responsible for the development and implantation of the security and privacy policies and procedures for the organization. Even though a facility might name an individual, that person may not have the expertise to implement the Security Rule provisions appropriately. In one study of small medical practices, the lack of expertise was the most commonly reported barrier to having an information security policy [27].

P4: The availability of IT expertise will affect compliance behavior.

Enforcement Environment

Classic deterrence theory posits that compliance occurs if the probability of swift detection and sanction in combination with the amount of the penalty outweighs the benefits of noncompliance. Therefore, some significant level of legal enforcement is essential for generating and assuring regulatory compliance. Enforcement is important for communicating regulatory norms and threatening credible levels of monitoring and legal sanctions for noncompliance. The enforcement environment comprises several factors that could affect Security Rule compliance.

Enforcement strategy. HITECH requires self-reporting of breaches and added significant strength to Security Rule enforcement above and beyond the original HIPAA enforcement scheme. Some studies focused on the effect of regulatory deterrence have shown that formal changes in levels of sanctions such as this, do change, at least for a while, the behavior of regulatees [37, 42]. Therefore, we posit that the changes made by HITECH will, at least in the short term, influence compliance behaviors.

P5: The more strict enforcement strategy of HITECH will affect Security Rule compliance behavior.

Risk of punishment. Although exact numbers are not available, most Security Rule violations are resolved voluntarily [43]. Only more serious violations result in fines and additional punishments. However, a facility cannot be certain that a data breach or other Security Rule violation will go unpunished if it cannot prove reasonable diligence to implement PHI protections. It is important to note that most of these violations are identified by complaints filed with the OCR. In a 2013 government report, OCR was criticized for not conducting audits at all, but rather focusing solely on "the complaint-driven approach" [36, p. 12]. Therefore, even though a facility should weigh the risk of possible punishments for noncompliance, some facilities may not perceive the risk as worthy of dedicating resources to properly secure PHI because the likelihood of being audited or investigated is small.

P6: The perceived level of risk of punishment will affect Security Rule compliance behavior.

Social and Normative Pressures

The general purpose of regulation, and therefore compliance, is reducing harm. The purpose of the Security Rule is to reduce potential harm that can be caused by exposure of PHI. However, regulation also has a socio-cultural purpose of reassuring citizens about the preservation of social order. Sociological studies have shown that changes in environmental norms and values in society, or changes in professional norms within an industry, likewise change the behavior of regulatees [39, 45]. The regulation of PHI is an important message for patients that offers assurance that their identities should be protected by healthcare providers and others. At the same time, the environmental norms related to information security are changing with new and growing security threats discovered continuously. These societal norms may motivate facilities to become fully Security Rule compliant.

Patient awareness/concern. Organizational theorists argue that organizations must comply with public expectations to build a reputation of legitimacy [11]. Further, trust in the organization will erode if the organization's actions do not meet public expectations [30]. Related to information security, consumer awareness of threats is increasing due to numerous high profile data breaches that have occurred such as those with Target Corporation [41] and Anthem, Inc. [28]. As a result, public expectations and concern about organizations protecting their data is high. In healthcare, a recent government survey revealed that 75% of individuals were concerned about the privacy of their medical records and 69% were concerned about the security of those records [33]. As consumers of healthcare, patients are likely to become more aware of the potential threat to their personal PHI, and it is unlikely that those potential threats will lessen any time soon. Therefore, pressures from a more aware patient population may impact a facility's compliance behaviors.

P7: The level of patient concern for potential security threats will affect Security Rule compliance behavior.

Stakeholder approval/concern. The Security Rule applies to CEs and their business associates. However, a healthcare facility has a number of stakeholders in addition to these entities and to patients that could be impacted in the event of a PHI breach. While CEs include some health providers, health plans, and healthcare clearinghouses, business associates can encompass a much larger network of stakeholders. This group of stakeholders might include legal and accounting service providers, financial institutions, consultants, and others. Many of these stakeholders may share electronic data as part of the healthcare supply chain. A review of several studies revealed that large companies' exposure to risks, including risks to information security, appeared to increase by having small organizations in the supply chain. Additionally, risk exposure for small organizations also increased [13]. Regardless of size, it is reasonable to expect that stakeholders in the healthcare supply chain could potentially pressure a facility to be in compliance with Security Rule requirements.

P8: The level of stakeholder concern about Security Rule compliance will affect compliance behaviors.

Moral duty. Researchers argue that the basic deterrence model is insufficient to allow for the effect of individual motivations and that moral obligation can help to explain compliance behavior. More specifically, the willingness to comply via moral duty occurs as long as the regulations are implemented by legitimate authorities [40]. In the case of the Security Rule, the legitimate authority is the U.S. government. Therefore, it is reasonable to consider that some degree of compliance behaviors will occur due to feelings of moral obligation on the part of the physician, office manager, or other staff. As healthcare providers, many individuals will work to protect PHI and display

compliance behaviors simply because it is the right thing to do and because the regulation stems from a legitimate source.

P9: The level of perceived moral obligation to protect PHI will affect Security Rule compliance behaviors.

Demographic and Organization Factors

In addition to resources, enforcement schemes, and social and normative pressures, some organizational factors will likely play a role in a facility's level of Security Rule (non)compliance behaviors. Three such factors are presented in this framework.

Facility size. Some studies report that small businesses in general have limited understanding of information security, technologies, and controls, and fail to perform risk assessment or create security policies [10, 15]. Others found that small organizations were less likely to implement preventive measures when compared to larger organizations [24]. In healthcare, results are similar; for example, one study reports that 33 percent of small provider respondents had never conducted a security risk assessment [19] and others report an alarming number of small medical practices without any security policy and procedures [27]. Size might be measured by the number of physicians, number of employees regularly in contact with PHI, number of patients served, or the number of CE, business associate, and other connections. Although this framework is focused on small facilities, even smaller subsets of size might be a determinant of (non)compliance behavior.

P10: The size of the facility will affect Security Rule compliance behavior.

Facility Type. The type of healthcare facility may also influence the level of compliance and noncompliance behaviors. Different types of facilities may be subject to different and greater threats. For example, many healthcare facilities face increased difficulty protecting data because medical equipment is often serviced through the Internet [25]. Examples of such equipment include dialysis and imaging machines which are often housed in small stand-alone facilities. Perhaps, due to the networked aspect of the medical equipment, these facilities would be more likely to be Security Rule compliant. As another example, nursing homes might be subject to more external scrutiny than other types of facilities through required state inspections. Therefore, nursing homes might be more likely to insure Security Rule compliance. Further, potential PHI threats may be more likely due to the nature of the facility, i.e. nursing home residents with many visitors. Due to the increased opportunity for access to PHI, a nursing home may be more cognizant of the need to comply with Security Rule provisions.

P11: The type of facility will affect Security Rule compliance behavior.

Management systems. Management systems provide a structure for getting work done properly and include processes and procedures to accomplish work efficiently and effectively. The lack of management systems and structure has been recognized as a barrier to regulatory compliance in healthcare and other industries [6, 46]. The absence of formal management systems within small businesses can contribute to information security problems since there may not be regular staff meetings, training, or formal monitoring systems in place. In small medical practices, particularly solo practices, systems and structure are dependent on the owner's skills and efforts since it is hard to attract professional management to that setting [9]. Therefore, the lack of formal management systems may impede full Security Rule compliance.

P12: The level of formality in management systems will affect Security Rule compliance behavior.

DISCUSSION AND CONCLUSION

The protection of personal information, and especially PHI, is a critical issue for healthcare organizations of all sizes. The HIPAA Security Rule was designed to insure that U.S. citizens' electronic health data is protected from loss or abuse. Nevertheless, studies have revealed that even large facilities may find it difficult to be fully compliant with the Security Rule. At the same time, evidence shows that small organizations face even more difficulties than large ones in obtaining resources which, in turn, may affect regulatory compliance in small healthcare facilities. This

is not an inconsequential problem since the abuse of PHI can result in a myriad of hardships for an individual. Therefore, it is imperative that the problem be addressed in a manner that can lead to improved compliance performance in small healthcare facilities.

In an effort to address the noncompliance issue, we must first understand the barriers that may prevent full Security Rule compliance. Toward that end, this paper describes a theoretical framework for explaining HIPAA Security Rule (non)compliance behaviors in small healthcare facilities. As part of the framework, twelve propositions are offered that summarize the theoretical arguments and that are designed to be tested in future empirical research. A key limitation of this work is that it is not necessarily a complete framework. There are likely many additional factors that affect Security Rule compliance. However, testing of these propositions should shed light on some of the difficulties that small facilities face, and thus lead to interventions that can aid in achieving Security Rule compliance. Although full compliance does not guarantee PHI protection, it greatly diminishes the chance that PHI will be exposed or abused.

This paper contributes to the literature in several areas including regulatory compliance, information security behavior, and healthcare policy. One implication for research is the provision of a theory-supported framework from which researchers may expand or design empirical tests.
Future empirical results will likely have important implications for theory and practice by identifying factors and interventions important to the protection of PHI in small healthcare facilities.

REFERENCES

1. American Recovery and Reinvestment Act of 2009. (2009). Pub. L. No. lll-5.
2. 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.
3. 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.
4. Brady, J. W. (2011). Securing health care: Assessing factors that affect HIPAA security compliance in academic medical venters. Proceedings of the *2011 44th Hawaii International Conference on System Sciences*, Manoa, Hawaii.
5. Brehm, J., & Hamilton, J.T. (1996). Noncompliance in rnvironmental teporting: Are biolators ignorant, or rvasive, of the law? *American Journal of Political Science, 40*(2), 444-477.
6. Cannoy, S. D., & Salam, A. F. (2010). A framework for health vare information sssurance policy and compliance. *Communications of the ACM, 53*(3), 126-131.
7. Chang, S. E., & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems, 106*(3), 345-361.
8. Coombs, F. S. (1980). The bases of noncompliance with a policy. *Policy Studies Journal, 8*(6), 885-892.
9. Denning, J. J. (2011). What's the best size for a practice? *UnCommon Sense*. http://www.medscape.com/viewarticle/739581
10. Dimopoulos, V., Furnell, S., Jennex, M., & Kritharas, I. (2004). Approaches to IT security in small and medium enterprises. Proceedings of the *2nd Australian Information Security Management Conference*. Perth, Western Australia.
11. Elsbach, K. D., & Sutton, R.I. (1992). Acquiring organizational legitimacy through illegitimate actions: A marriage of institutional and impression management theories. *Academy of Management Journal, 35*(4), 699-738.
12. Etienne, J. (2011). Compliance theory: A goal framing approach. *Law & Policy, 33*(3), 305-333.
13. Finch, P. (2004). Supply chain risk management. *Supply Chain Management: An International Journal, 9*(2), 183-196.
14. Graham, C. M. (2010). HIPAA and HITECH compliance: An exploratory study of healthcare facilities ability to protect patient health information. Proceedings of the *Northeast Business & Economics Association*. Montclair, New Jersey.
15. Gupta, A., & Hammond, R. (2005). Information systems security issues and decisions for small businesses: An empirical examination. *Information Management & Computer Security, 13*(4), 297-310.
16. Haeussinger, F. and Kranz J. (2013). Understanding the antecedents of information security awareness: An empirical study. Proceedings of the *Nineteenth Americas Conference on Information Systems*. Chicago, IL.

17. Health Information Technology for Economic and Clinical Health. (2013). 78 Fed. Reg. 5566
18. Health Insurance Portability and Accountability Act of 1996. (1996). Pub. L. No. PL 104-191, 100 Stat. 2548 Stat.
19. Healthcare Information and Management Systems Society. (2011). *Privacy and security toolkit for small provider organizations*. Available: http://www.himss.org/library/healthcare-privacy-security/small-provider-toolkit?navItemNumber=16493
20. HIPAA Breach Notification Rule, 45 CFR 165.400-414 (2009).
21. HIPAA Privacy Rule, 45 CFR 164 (2003).
22. HIPAA Security Rule, 45 CFR 164 (2005).
23. Kane, C. K., & Emmons, D. W. (2013). *New data on physician practice arrangements: Private practice remains strong despite shifts toward hospital employment.* Chicago, IL: American Medical Association. Available: http://www.nmms.org/sites/default/files/images/2013_9_23_ama_survey_prp-physician-practice-arrangements.pdf
24. Kankanhalli, A., Teo, H. H., Tan, B. C. Y., & Wei, K. K. (2003). An integrative study of Information Systems security effectiveness. *International Journal of Information Management, 23*(2), 139-154.
25. King, R. (2014, February 18). Nursing homes are exposed to hacker attacks. *The Wall Street Journal*. Available: http://www.wsj.com/articles/SB10001424052702304899704579389171658671940
26. Knapp, K. J., & Ferrante C. J. (2014). Information security program effectiveness in organizations: The moderating role of task interdependence. *Journal of Organizational and End User Computing*, *26*(1). 27-46.
27. Martin, N. L., & Imboden, T. R. (2014). Information security and insider threats in small medical practices. Proceedings from the *Twentieth Americas Conference on Information Systems.* Savannah, GA.
28. Mathews, A.W., & Yadron, D. (2015, February 4). Health insurer Anthem Hit by hackers. *The Wall Street Journal*. Available: http://www.wsj.com/articles/health-insurer-anthem-hit-by-hackers-1423103720
29. Mishra, S., Leone, G.J., Caputo, D.J., & Calabrisi, R.R. (2011). Security awareness for health care Information Systems: A HIPAA compliance perspective. *Issues in Information Systems, XII*(1), 224-236.
30. Murray, K. B., & Vogel, C. M. (1997). Using a hierarchy-of-effects approach to gauge the efectiveness of corporate social responsibility to generate Goodwill toward the firm: Financial versus nonfinancial impacts. *Journal of Business Research, 38*(2), 141-159.
31. Nielsen, V. L., & Parker, C. (2008). To what extent do third parties influence business compliance? *Journal of Law & Society, 35*(3), 309-340.
32. Nielsen, V. L., & Parker, C. (2012). Mixed motives: Economic, social, and normative motivations in business compliance. *Law & Policy, 34*(4), 428-462.
33. Patel, V. (2014). *Trends in national perceptions regarding privacy and security*. Office of the National Coordinator for Health Information Technology.
34. Redspin. (2014). *Redspin's Breach Report 2013: Protected health information (PHI)*. Carpinteria, CA. Available: http://www.redspin.com/resources/whitepapers-datasheets/2013-Breach-Report-Protected-Health-Information-PHI-Redspin.php
35. Rindfleisch, T. C. (1997). Privacy, information technology, and health care. *Communications of the ACM, 40*(8), 93-100.
36. Salmon, T. M. (2013). *The Office for Civil Rights did not meet all federal requirements in its oversight and enforcement of the Health Insurance Portability and Accountability Act Security Rule*. (A-04-11-05025). Available: https://oig.hhs.gov/oas/reports/region4/41105025.pdf
37. Scholz, J. T. (1997). Enforcement policy and corporate misconduct: The changing perspectives of deterrence theory. *Law and Contemporary Problems, 60,* 253-268.
38. Schmidt, R. A., Bennison, D., Bainbridge, S., & Hallsworth, A. (2007). Legislation and SME retailers: Compliance costs and consequences. *International Journal of Retail & Distribution Management, 35*(4), 256-270.
39. Simpson, S. S. (2002). *Corporate crime, law, and social control*. Cambridge: Cambridge University Press.
40. Sutinen, J. G., & Kuperan, K. (1999). A socio-economic theory of regulatory compliance. *International Journal of Social Economics*, *26*(1/2/3), 174-193.
41. Target. (2013). *Target confirms unauthorized access to payment card data in U.S. stores*. Retrieved from http://pressroom.target.com/news/target-confirms-unauthorized-access-to-payment-card-data-in-u-s-stores
42. Tittle, C. (1980). *Sanctions and social deviance: The question of deterrence.* New York: Praeger.
43. U.S. Department of Health & Human Services. (n.d.). *How OCR enforces the HIPAA Privacy & Security Rules.* Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/enforcement/process/index.html

44. Warkentin, M., Johnston, A. C., & Adams, A. M. (2006). User interaction with healthcare Information Systems: Do healthcare professionals want to comply with HIPAA? *Proceedings of the Twelfth Americas Conference on Information Systems*, Acapulco, Mexico.
45. Winter, S., & May, P. (2002). Information, interests, and environmental regulation. *Journal of Comparative Policy Analysis, 4*(2), 115.
46. Yapp, C., & Fairman, R. (2006). Factors affecting food safety compliance within small and medium-dized Enterprises: Implications for tegulatory and rnforcement dtrategies. *Food Control, 17*, 42-51.

APPENDIX A