2016

Examining Data Privacy Breaches in Healthcare

Tanshanika Turner Smith
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Tanshanika Turner Smith

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Gergana Velkova, Committee Chairperson, Doctor of Business Administration Faculty

Dr. David Moody, Committee Member, Doctor of Business Administration Faculty

Dr. Roger Mayer, University Reviewer, Doctor of Business Administration Faculty

Chief Academic Officer
Eric Riedel, Ph.D.

Walden University
2016

Abstract

Examining Data Privacy Breaches in Healthcare

by

Tanshanika T. Smith

MBA, Southern Polytechnic State University, 2003

MS, Southern Polytechnic State University, 2002

BBA, Georgia State University, 1998

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

August 2016

Abstract

Healthcare data can contain sensitive, personal, and confidential information that should remain secure. Despite the efforts to protect patient data, security breaches occur and may result in fraud, identity theft, and other damages. Grounded in the theoretical backdrop of integrated system theory, the purpose of this study was to determine the association between data privacy breaches, data storage locations, business associates, covered entities, and number of individuals affected. Study data consisted of secondary breach information retrieved from the Department of Health and Human Services Office of Civil Rights. Loglinear analytical procedures were used to examine U.S. healthcare breach incidents and to derive a 4-way loglinear model. Loglinear analysis procedures included in the model yielded a significance value of 0.000, $p > .05$ for the both the likelihood ratio and Pearson chi-square statistics indicating that an association among the variables existed. Results showed that over 70% of breaches involve healthcare providers and revealed that security incidents often consist of electronic or other digital information. Findings revealed that threats are evolving and showed that likely factors other than data loss and theft contribute to security events, unwanted exposure, and breach incidents. Research results may impact social change by providing security professionals with a broader understanding of data breaches required to design and implement more secure and effective information security prevention programs. Healthcare leaders might affect social change by utilizing findings to further the security dialogue needed to minimize security risk factors, protect sensitive healthcare data, and reduce breach mitigation and incident response costs.

Examining Data Privacy Breaches in Healthcare

by

Tanshanika T. Smith

MS, Southern Polytechnic State University, 2003

BBA, Georgia State University, 1998

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

August 2016

Dedication

I would like first to thank God for giving me the never-ending attitude, courage, and strength to complete this journey. I also thank God for giving me supportive family and friends whom I needed, relied, and leaned on at varying times to complete this journey. I am truly blessed and humbly thankful for all of God's many blessings. I dedicate the entire manuscript to my family and extended family who sacrificed so much for me to get to this point, thank you from the depth of my heart. Either words or actions can ever express the sincere appreciation, love, and support that I have for each one of you. All of you form the foundation for which I stand. I am forever grateful for your many sacrifices and all that you have done for me. I never would have accomplished my goal without the hard work, support, dedication, and countless sacrifices from all of you. Without your many efforts, constant encouragement, helping hands, and never-ending support, I could not have achieved this goal. From humble beginnings, all of my many blessings flow thank you!

Acknowledgments

To my outstanding, kind, and magnificent dear husband and my wonderful loving yet phenomenal children you are the glue that kept me going. Thank you, thank you, thank you, for everything that you have done to help me reach my goal you all are truly amazing. I am so honored, proud, and blessed to have family members such as each of you. Thank you for allowing me time to lock myself in the office and work at times when I know that it was very inconvenient for everyone. You all mean the world to me, and I love and cherish you very much. Thank you for challenging and encouraging me to complete this journey. To my immediate and extended family, thank you for everything that you have done for me. I appreciate all the acts of kindness and love shown to me. Family means so much to me, without your support, I could not have achieved this goal. Each and everyone one of you played an integral role in my success. Based on your collective efforts, I am everything that I am. I could not have reached this point without all of you. Words can never express the sincere appreciation, thoughtfulness, and honor that I have for each of you. I love you and cherish you from the depth of my soul. To the entire Walden faculty who poured so much knowledge into me, and especially my chair who guided me along this scholarly journey, I am forever grateful for the help and support that you gave me. Without each of you challenging me to reach for higher heights, I would have never reached my goal, thank you so much for the scholarship and service you gave me.

Table of Contents

List of Tables

List of Figures

Section 1: Foundation of the Study

Information assets are critical resources that managers rely upon to conduct business and how well entity leaders can effectively protect, secure, and manage data affect organizational survival (Dzazali & Zolait, 2012). Information security encompasses many broad areas, and some scholars may approach information security research from technological perspectives such as intrusion detection, user provisioning, access controls, and encryption (Dzazali & Zolait, 2012). Although technological aspects of security research could be of importance to business leaders, examining information security from a breach management and privacy perspective may be equally important to managers. Included in this section is an overview of the importance of examining information security risks, threats, and the potential effects of ineffective security management on business survival.

Effective security strategies can lead to reputational benefits, cost savings, and reduce incident response times (Abu-Musa, 2010). However, failing to implement adequate security can affect an organization's competitive position (Abu-Musa, 2010). Customers of various global enterprises expect business leaders to safeguard their sensitive data (Sauls & Gudigantala, 2013). Breach prevention and information security management are vital to organizational success (Chang & Wang, 2011; Sauls & Gudigantala, 2013) as organization leaders utilize and rely on information systems to run their businesses (Chang & Wang, 2011).

Due to significant monetary losses resulting from data breaches, organizational managers have shifted priorities and information security budgets (Chang & Wang,

2011). Damages and losses resulting from the effects of data breaches are costly to organizations (Wall, 2013). Web-based solutions, remote, and mobile technologies can increase information security risks and potential threats (Kruger & Mama, 2012). Data breaches are one of the most critical security risks business leaders face costing organizations approximately $7.2 million in 2011 signaling a growing need for researchers to investigate these issues (Ayyagari, 2012). A data breach happens when disclosures or unauthorized access to sensitive or personal information occur (Roberts, 2014). Generally, data breaches relate to one of three broad categories: (a) *confidentiality breaches,* which are attempts to acquire or gain access to sensitive data; (b) *integrity breaches*, incidents related to the modification, change, or altering of data, or (c) *availiability breaches*, security events resulting in downtime, disruption, or system outages (Chen, Li, Yen, & Bata, 2012). In some industries, breaches are decreasing, but in the healthcare and medical sectors, the number of attacks is rising (Ayyagari, 2012). Thus, business leaders must implement defensive strategies to protect against growing vulnerabilities by addressing both technological and human threats (Selamat & Babatunde, 2014).

Background of the Problem

In response to growing public concern, fears of unwanted data exposure, and a changing regulatory climate, healthcare practitioners must ensure medical information is secure and protected (Kwon & Johnson, 2013). Medical data contains some of the most sensitive information about an individual, such as (a) name, (b) date of birth, (c) address, (d) other personal identifying information, (e) details regarding specific medical

problems, (f) individual diagnosis of addiction related health issues, (g) treatments, (h) medications, (i) financial, and (j) insurance information (Kamoun & Nicho, 2014). In the United States, both governmental and business leaders have used various strategies to prevent data breaches (Sen & Borle, 2015). Some actions taken to prevent data breaches include the passage of breach notification laws, increased spending to fund security initiatives, and mandated data privacy requirements, but breach incidents continue to occur (Sen & Borle, 2015). Organizational leaders may be underprepared to manage security issues and totally eliminate information security threats (Selamat & Babatunde, 2014). However, businesses should implement adequate safeguards to secure and appropriately manage their data from growing potential exploits, threats, and vulnerabilities (Selamat & Babatunde, 2014). Therefore, to better equip medical and techology practitioners with information that they might use to implement adequate safeguards and to manage security threats, healthcare leaders, may need to understand the relationship between various factors that might contribute to data breaches (Taylor & Robinson, 2015).

Problem Statement

Data breaches can lead to legal exposure (Adler, Demicco, & Neiditz, 2015), financial harm, and reputational damage (Adler et al., 2015; Wikina, 2014), resulting in provider and business associates losses (Sacopulos & Segal, 2014). In 2012, approximately two-thirds of breaches were related to errors and system malfunctions and roughly 47% of breaches represented theft and hacking (Srivastava & Kumar, 2015). Accidental loss resulting from device theft represented approximately 77% of healthcare

breaches in 2014 (Roberts, 2014) and nearly 30% of breaches involved business associates (Wikina, 2014). Annually, cybercrime costs consumers billions (Roberts, 2014) and breaches cost organizations nearly $7 billion (Williams & Hossack, 2013). The general business problem is that breaches can result in legal, financial, and reputational damages. The specific business problem is that some healthcare practitioners do not understand the association between data privacy breaches, business associates, covered entities, the number of individuals affected, and data storage locations.

Purpose Statement

The purpose of this quantitative loglinear study was to examine the association between data privacy breaches, business associates, covered entities, the number of individual affected, and data storage locations. The variables were data privacy breaches, covered entity types, number of individuals affected, storage location of breach data, and business associates. The study took place in Atlanta, Georgia, and the population included secondary data related to breach incidents reported by healthcare leaders across the United States in years 2009 to 2016. Findings from this research could provide healthcare practitioners and other business professionals with knowledge, information, and understanding of relationships associated with data privacy breaches. Healthcare leaders might use information from this study to change business practices, implement appropriate preventative measures, and manage data security effectively. Contributions to social change might include healthcare practitioners utilizing the findings and recommendations from this study to improve and better secure private medical records of patients and individuals. Another contribution to social change might include healthcare

leaders utilizing the findings presented in this study to minimize data security risk factors, protect sensitive healthcare data, and reduce costs associated with breach mitigation and response activities.

Nature of the Study

Quantitative researchers focus on specific research questions and use numerical data to answer a research question (Farrelly, 2013). The most appropriate research method for this study was the quantitative research approach because I formulated a specific research question and used numerical means to answer a research question. Researchers use qualitative techniques to uncover and explore in-depth meanings and interpretations of individual life experiences about a particular phenomenon (Birchall, 2014). Conversely, mixed method researchers integrate aspects of both qualitative and quantitative research techniques to understand multifaceted phenomenon via many different perspectives (Gambrel & Butler, 2013; Long, 2014) and to analyze complex issues involving multilevel processes and systems (Fetters, Curry, & Creswell, 2013). The purpose of this study was not to explore phenomenon and uncover in-depth individual meanings. Therefore, a qualitative research approach was not appropriate for this study. Mixed methods research was not appropriate for this study because the goal of this study was not to combine different approaches to understand complex multilevel or multifaceted phenomenon and processes.

The selected design for this study was a loglinear research design. Researchers use correlational designs to identify and examine relationships that may exist among variables (Holosko, Jolivette, & Houchins, 2014). Loglinear approaches are appropriate

techniques that researchers can use to analyze relationships between categorical variables (Vaid, 2012). In this study, I analyzed the relationships between categorical variables. Thus, a loglinear design was an appropriate design for this study. In experimental designs, researchers use randomization, a control group, and manipulation, or in quasi-experimental designs, researchers may omit one of these elements to determine variable relationships (Sousa, Driessnack, & Mendes, 2007). The goal of this study was not to utilize control groups, randomization, and manipulation to predict relationships between variables, thus neither an experimental nor a quasi-experimental design was appropriate for this study.

Research Question

Research questions should be specific and formulated based upon solid theoretical analysis (Weller et al., 2012). Some considerations for developing research questions include the feasibility, practicality, and relevancy of the research both to the individual researcher and scientific community at large (Ajithkumar, 2012). A scientific research question should be testable, appropriate for data collection and empirical analysis, and lead to a potential answer (Graves & Rutherford, 2012). There should be consistency between the title of the work, the purpose and problem statement, and the research question (Newman & Covrig, 2013). The research question related to this study was:

> RQ: What is the association between data privacy breaches, data storage locations, business associates, covered entities, and number of individuals affected?

Hypotheses

The hypothesis is an informed guess or statement and categorization about how things work (Bettany-Saltikov & Whittaker, 2014). The research hypothesis is an integral component of a well-crafted research study and is the foundation of the overall study (Toledo, Flikkema, & Toledo-Pereyra, 2011). Although there is no single best approach to testing a hypothesis, the hypothesis must be appropriate for the research and scholars should consider various factors when determining the hypothesis (Bettany-Saltikov & Whittaker, 2014).

Research hypotheses should be appropriate, carefully crafted, and based on facts, ideas, or observations grounded in the research (Toledo et al., 2011). Often described as deductive, inductive, directional, non-directional, alternative, and null, the research hypothesis is a clear articulation of the perspective that researchers use to highlight the essence of the research problem (Toledo et al., 2011). Scholars form their hypothesis on prior research or the literature and may develop either a simplistic or complex hypothesis (Toledo et al., 2011). The hypotheses for this study were as follows:

> $H_0$1: There is not an association between data privacy breaches, data storage locations, business associates, covered entities, and number of individuals affected by a data breach.
>
> H_a1: There is an association between data privacy breaches, data storage locations, business associates, covered entities, and number of individuals affected by a data breach.

Theoretical Framework

A theoretical framework is the integration and synthesis of ideas and concepts that researchers identify in an attempt to explain, describe, or predict a certain phenomenon and guide their work (Green, 2014; Imenda, 2014). Developed in 2003, by Hong, Chi, Chao, and Tang, integrated system theory of information security management was the theoretical framework that served as the basis for this study. Hong et al. (2003) developed this theory to address the gaps, limited depth, and omissions of other information management theories. Hong et al. (2003) integrated and combined aspects of prior theories related to policy, risk, internal controls management, and contingency planning. Integrated system theory consists of elements or constructs relating to functions of information security management, internal control, and contingency management (Hong et al., 2003).

Abu-Musa (2010) used integrated system theory to evaluate, understand, assess, and analyze security and governance practices that led to business success. Similarly, I used integrated system theory as the theoretical framework to guide my research as I sought to understand the relationships between data privacy breaches, business associate involvement, medical entity types, breach location, record exposure, and theft. Integrated system theory is a comprehensive framework researchers can use to guide empirical studies (Hong, Chi, Chao, & Tang, 2006). Using integrated system theory, researchers can examine organizational management practices, behaviors, and activities related to information security (Hong et al., 2006). Integrated system theory was an appropriate framework for this study, and I used this theory to understand the relationships between

data privacy breaches, theft, business associate involvement, medical entity types, breach location, and record exposure.

Definition of Terms

Operational definitions used in research may vary depending on individual expertise and judgment (Jing, Brockett, Golden, & Guillén, 2013). Scholars may develop operational definitions at the onset of the research process to inform and provide readers with standard terminology, meaning, and interpretation for certain constructs used in their research (Hanson-Abromeit & Moore, 2014). Outlined below are operational definitions used in this study. The purpose of these definitions is to provide readers with certain understanding of concepts and terminology within the field of information security used in the context of this study.

Breach: A breach is the unauthorized access or violation of an established set of norms, rules, and standards (Liu, Musen, & Chou, 2015), or an inappropriate, improper release, disclosure, access, or nonpermitted usage of an individual's personal health information that could result in unwanted consequences and outcomes to the individual such as financial or reputational harm, or which might cause any other form of damages and harm (Cascardo, 2012; Sterling, 2015; Wikina, 2014).

Business associates: The term healthcare professionals use to describe business partners and cooperative organizations such as vendors, contractors, and service providers who process, manage, receive, transmit, create, or maintain personally identifiable information or protected health data while acting on behalf of the covered health entity (Amundson & Cole, 2013).

Covered entity: An organization such as a health plan, clearinghouse, or medical provider that electronically transmits, facilitates, coordinates, processes, or handles medical and health related information (Flaherty, 2014).

Data breach: A data breach is a type of security incident that involves the inappropriate usage, access, acquisition, or compromise of any sensitive, protected, or confidential data (Adebayo, 2012; Chen et al., 2012) or that results in the unauthorized disclosure of an individual's sensitive or personal information (Romanosky, Hoffman, & Acquisti, 2014).

Health information technology for economic and clinical health (HITECH) act: Passed by the U.S. Congress in 2009, the HITECH law includes provisions for mandatory reporting and notification requirements for breaches of healthcare information (Liu et al., 2015).

Health insurance portability accountability act (HIPAA): Signed into law by President Bill Clinton in 1996, the overall purpose of the HIPAA law includes improving health insurance coverage, simplifying healthcare administration, reducing the occurrences of fraudulent misuse, waste, and abuse of information, and facilitating easier access to health saving accounts and long-term care services (Jacques, 2011).

Personal health information: Personal health information is protected medical records and associated data retained, transmitted or maintained electronically, or kept in any form or media which contains personally identifiable information about an individual or information that is specifically relates to a particular person (Jacques, 2011).

Threat: This term broadly means any possible harm or damage resulting from the inappropriate misuse or abuse of protected information assets (Haley, Laney, Moffett, & Nuseibeh, 2006).

Assumptions, Limitations, and Delimitations

Scholars might highlight and discuss assumptions, limitations, and delimitations in their work. Assumptions are inherently predicated or perceived truths or beliefs related to the study that the researcher discloses (Dean, 2014). Assumptions refer to researchers' individually held or deeply rooted system of thoughts, beliefs, feelings, and perceptions that may not always be obvious and easily recognized (Markette, 2012). Scholars have certain individual assumptions and belief systems that may influence their worldview or understanding of a phenomenon (Bradt, Burns, & Creswell, 2013). Conversely, limitations are inherent weaknesses of a study, and delimitations refer to the specific restrictions or sample populations researchers choose in their studies (Brughelli, Cronin, Levin, & Chaouachi, 2008). Delimitations are purposeful restrictions the researcher imposes on the design of a study (Dean, 2014).

Assumptions

Researchers also describe assumptions underlying truths, beliefs, realities, or ideas (Bradt et al., 2013; Dean, 2014; Roy, 2014) relating to the fundamental characteristics of a study (Dean, 2014). Assumptions can affect how researchers disseminate knowledge and conduct scientific inquiry (Ketsman, 2012). Alvesson and Sandberg (2011) noted that the five main areas of assumptions are in-house, root metaphor, paradigm, field, and ideology. In-house, paradigmatic, and ideological

assumptions typically relate to certain characteristics that apply to the research. Root metaphor assumptions relate to general images or classifications of a subject matter (Alvesson & Sandberg, 2011). Paradigmatic assumptions are characteristics or components that are critical to the overall meaning of a subject matter, and the absences of these necessary components might devise an entirely new meaning (Alvesson & Sandberg, 2011). Ideology assumptions are those factors relating to a researcher's core beliefs and values. These include political, moral, and gender beliefs that may influence the researchers' perspective (Alvesson & Sandberg, 2011). Field assumptions are broad overarching traits or relevant views collectively shared, set aside, or otherwise related solely to a particular discipline or area (Alvesson & Sandberg, 2011). Researchers should disclose assumptions related to their work in a clear, open, transparent, and honest manner because assumptions are an integral and necessary aspect of scientific inquiry (Nelson, 2012).

Assumptions related to this study were that information regarding actions and countermeasures contained in the data breach reports were accurate and comprehensive. Another assumption was that individuals who submitted the data breach reports had appropriate knowledge relating to the specific countermeasures and actions that entity leaders took in response to the data breach. Also assumed was that knowledgeable individuals accurately completed the report and included all relevant and pertinent information about the countermeasures and details relating to the breach incident. Several states within the United States have adopted some form of notification laws relating to data privacy breaches (Romanosky, Acquisti, & Telang, 2011). The consequences of not

complying with notification laws could include civil action resulting in massive fines and penalties (Romanosky et al., 2011). In terms of penalty, some state laws do not have limits or restrictions on the dollar amount of penalties and awards (Romanosky et al., 2011). Additionally, state attorneys general could take additional actions against entities that fail to comply with notification laws (Romanosky et al., 2011). Thus, I assumed that the threat of penalty and negative enforcement actions that may occur if healthcare officials fail to comply with state notification laws helps to ensure and mitigate the risk that information may be potentially inaccurate, or incomplete. Due to the possibilities of penalties, I also assumed that it is likely that knowledgeable individuals reported accurate and sufficient breach information. Therefore, I assumed that the likelihood that incident reports are inaccurate or include irrelevant information is relatively low and assume that the dataset used for this study contains comprehensive, adequate, and appropriate data for this research.

Limitations

Limitations refer to systematic occurrences or factors beyond the researcher's control that affect either the internal or external validity of a study (Price & Murnan, 2004). Limitations are weaknesses of the study researchers disclose to help readers understand the context and validity of the work regarding creditability of conclusions reached during the study (Breaux, Black, & Newman, 2014; Dean, 2014). Researchers may fail to highlight limitations for many reasons that include inadequate knowledge or skills, unfamiliarity with research practices, lack of training, the desire to influence readers by omitting information that can change a reader's view of a particular study, or

the overall belief that readers should simply be aware of limitations (Price & Murnan, 2004).

A limitation of this study was that leaders of covered entities may misreport to United States Department of Health and Human Services (DHHS) estimated information relating to the exposure incident. Examples of possible misreported data might include estimates for the number of individuals impacted, assumptions about all of the various formats of the stored breached information resulting in data loss, and timeframe estimates related to the date that the breach incident occurred. Thus, the electronic DHHS breach repository may not contain all pertinent facts relating to the breach incident. Some state laws include provisions requiring entities to file an incident report and invoke notification obligations without any unnecessary delay once there is reasonable information revealed about an occurrence of inappropriate disclosure or access (Breaux et al., 2014). Thus, due to time constraints required under state disclosure laws, respondents may complete the incident report before regulators fully evaluate, review, and investigate the breach incident or may fail to report all pertinent facts of the incident until case details are known.

Another possible limitation of the study was that the data repository may not contain information about all privacy breach incidents covered under U.S. healthcare laws. DHHS disclosure requirements contain specific exclusions and reporting exemptions for some entities. Under the healthcare rules, entities are exempt from reporting requirements when the unsecured health data relating to a breach is unusable (Plunkett, 2013). Exclusions of breach reporting also are applicable when certain

technological features such as encryption result in the exposed data rendered unreadable or otherwise useless (Plunkett, 2013). Reporting exemptions exist when personal data is nonidentifiable (Wan et al., 2015) or there is a relatively low or unlikely possibility that breached data could lead to individual harm (Cascardo, 2014). Therefore, the dataset may not contain all information relating to breaches of sensitive health information affecting 500 or more individuals. However, the risk of under-reporting may be reduced because HIPAA notification requirements include mandates that individuals of both covered entities and business associates report disclosures of sensitive data or risk monetary fines (Johnson, 2014; McDavid & West, 2014; Weisse, 2014).

Delimitations

Delimitations refer to the predetermined or planned constraints (Sampson et al., 2014), scope, conceptual distinction, or boundary limits of a study that researchers use to clarify the specific parameters chosen for the study (Williams & Hossack, 2013). Delimitations are the actions that researchers perform to help manage the data (Ellis & Levy, 2009). Kamati, Cassim, and Karodina (2014) noted that delimitations are aspects of the study that researchers control or select for inclusion in the study. Researchers may delimit a study by restricting participation in a study to only participants who are members of certain ethnic or age groups or may limit study participants to only individuals who meet certain characteristics or traits the researcher desires (Price & Murnan, 2004). For this study, I delimited and restricted data analysis to breach incidents reported by U.S. healthcare professionals in years 2009 through the beginning of 2016. Within the 2009 to 2016 timeframe, I examined and reviewed all reports of privacy

breach cases contained in the online notification database that OCR officials previously evaluated and resolved. To help readers understand the boundaries and scope of the study, researchers note delimitations and outline what they plan to do in the study (Ellis & Levy, 2009). The scope of this study included all information related to data breach incidents investigated and closed by OCR officials since the passage of the HITECH law in 2009.

Significance of the Study

Security is a strategic business issue (Willey & White, 2013). Due to the rise in the number of data breach incidents, protecting data is a concern for leaders across various industries (Gatzlaff & McCullough, 2012). In response to data breaches and data protection failures, legislative reaction resulting in the proposal of new policies and laws has increased (Gatzlaff & McCullough, 2012). Additionally, expenses, costs, and human resources required to investigate, respond to, and mitigate issues associated with breach occurrences can be extensive for all parties involved in the incident (Gatzlaff & McCullough, 2012). Financial costs, fines, and penalties associated with breach incidents can be extensive even in cases of accidental data loss or when there is no clear indication of data misuse (Gatzlaff & McCullough, 2012). Governing authorities may impose fines on medical organizations for failing to protect data (Hayhurst, 2014). There could be additional costs associated with individual patient lawsuits; therefore, financial costs relating to healthcare data breaches can be substantial (Hayhurst, 2014).

Business leaders who manage information security risks may use the findings from this study to improve business practice. Organizational leaders might utilize

findings from this study to devise new approaches to managing strategic priorities associated with information security more effectively. Additionally, information about data breaches and possible relationships that may exist may lead to healthcare leaders developing better methods and solutions for protecting sensitive data and preventing data privacy breaches.

Contribution to Business Practice

Findings from this study may contribute to the existing body of literature relating to data privacy breaches. Lack of adequate staffing, ineffective response planning, and limited awareness of compliance rules contribute to organizational data breaches (Kieke, 2014). Information contained in this study could help healthcare practitioners understand the factors associated with data security risks and corresponding prevention strategies needed to minimize data privacy breaches. Security issues (Ahuja & Rolli, 2012) and data breaches (Vockley, 2012) can affect the entire healthcare industry (Ahuja & Rolli, 2012; Vockley, 2012) rather than a single individual, hospital, or entity (Vockley, 2012). Following a large data breach, there could be charges for credit monitoring, loss of staff productivity, external investigative reporting, and crisis intervention and management activities that costs organizations between $4 million and $7 million per incident. These costs include response costs that can total a few hundred thousand dollars (Claunch & McMillan, 2013).

Healthcare leaders might utilize the information contained in this study to improve data security and reduce organizational costs associated with security incident and breach response activities. Technology and healthcare practitioners might utilize the

findings from this study to gain a better understanding of the various relationship factors associated with data privacy breaches and managing data security. There could be provisions in some state laws that require companies to adhere to certain notification requirements when data breaches of personally identifiable information occur (Breaux et al., 2014). Study results may help leaders gain an understanding of particular approaches used by industry professionals that may be appropriate and needed to comply with specific state laws affecting their particular organization. Organizations need a detailed response plan and prevention strategy to manage data breaches (Breaux et al., 2014). Knowledge gained from this study could equip healthcare professionals with the information they need to devise appropriate plans to prevent data breaches of patient information.

Before an incident occurs, healthcare practitioners should perform extensive preplanning, establish forensically sound data collection practices, review key operational processes, and comprehensively examine organizational policies and procedures (Claunch & McMillan, 2013; Kerr, DeAngelis, & Brown, 2014). Findings from this study may help healthcare practitioners identify approaches they can use to develop adequate incident response plans. By developing effective response and mitigation plans, healthcare and technology professionals could perhaps strengthen organizational controls, identify appropriate countermeasures, and contribute to the sustained market value, long-term success, and viability of healthcare entities.

Data breaches can affect the reputation and financial outlook of firms (Wikina, 2014). Business leaders may find this study beneficial as information contained in this

study may help businesses avoid negative financial consequences and reputational damage associated with unwanted data breaches. Study findings may include relevant and useful information that healthcare practitioners and security professionals may need to protect and better secure patient data entrusted to their care. Knowledge regarding data breaches uncovered during this study may add to the broader field of breach management and information security research. Future researchers seeking an understanding of data prevention strategies and information security may find information gathered from this study useful.

Implications for Social Change

Companies should implement adequate safeguards and regular monitoring to minimize violations and breaches (Hayden, 2013). Implementing common technological strategies can reduce exposure risks and protect healthcare data (Hayden, 2013; Jenkins, 2013). The results of this study may positively affect social change by highlighting prevention strategies that healthcare organizations might use to protect the security, privacy, and integrity of individual health records. Breaches of healthcare data could have impacts that are more devastating on individuals than the impact of a credit card breach, as criminals who obtain personal, health, billing, and medical data can completely compromise a person's identity resulting in many variations of fraudulent transactions (McNeal, 2014). Fraudulent billing transactions account for a significant number or medical claims and services (Appari & Johnson, 2010). Data collected during this study may positively benefit society as a whole by minimizing the impact that data breaches could have on the lives of individuals, such as medical fraud, identity theft, and other

damage. Criminal acts of healthcare fraud and medical identity theft committed by perpetrators and hackers increased in the industry (Claunch & McMillan, 2013). The results of this study may have positive, practical implications for individuals, healthcare entities, and the medical industry as a whole, and could help to reduce the rate of medical and identity fraud.

A Review of the Professional and Academic Literature

Scholars use a variety of formats when presenting literature reviews that often include a systematic analysis and synthesis of existing literature related to a particular topic or phenomenon (Callahan, 2014). When conducting literature reviews, researchers become familiar with a topic, understand different theories, methods, and approaches scholars used in prior research on the topic, identify potential gaps within the existing body of literature, and uncover common challenges, themes, and issues regarding the subject matter (Pickering & Byrne, 2014). In literature reviews, writers evaluate, synthesize existing literature, and show the connections between prior scholarly works and their work to help justify the relevance and appropriateness of proposed studies (Kwan, Chan, & Lam, 2012). Presented in this literature review is a discussion of some theories that prior scholars used when conducting data breach research. This literature review also includes information about the theory chosen for this study. Topics that form the basis of this study relate to risks and possible effects of data breaches on individuals and organizations, as well as, possible reasons security incidents may be of relevant importance to professionals within the healthcare sector.

This literature review also contains information regarding some recently published empirical research studies on data breaches. Choosing the "all database" option within the ProQuest and Academic Search Complete databases of the Walden Library, I used search terms such as *data breach, privacy breach, security breach, security incident,* and *breach incident* to identify relevant articles for the literature review. I also enabled the related words feature of the ProQuest and Academic Search Complete database systems to identify relevant articles that were similar or closely related to the topic of data breaches. I also utilized the Google Scholar search engine to locate relevant information for this literature review. Within Google Scholar, I also limited search results to only articles published in 2011 and beyond. Finally, to identify articles for this literature review, I selected relevant articles and empirical studies geared towards information security management, information technology, information security threat mitigation, and risks prevention. Over 90% of the sources that I used in the resulting literature consist of peer-reviewed articles published since 2012.

Integrated System Theory

Constructs of integrated system theory are relevant in understanding security threats (Sharma & Sugumaran, 2011). Five theories form the basis of integrated system theory including (a) security policy, (b) risk management, (c) internal control and auditing, (d) management, and (e) contingency theory (Sindhuja, 2014). Aspects of integrated system theory relate to the hardware, software, technological, operational, and administrative processes used to protect and secure information resources (Ismail, Sitnikova, & Slay, 2014). Integrated system theory is an appropriate framework for

understanding information security outcomes, strategies, and organizational practices (Sharma & Sugumaran, 2011) and this theory is a broad framework that is appropriate for examining organizational decisions, activities, actions, and behaviors related to information security (Sindhuja, 2014). Integrated system security of information management framework includes security policy, risk management, auditing, and internal controls monitoring, which are strategic tools that leaders can use to manage effectively various information security issues within their organizations (Järveläinen, 2012). Organizational leaders can utilize and apply strategic concepts related to integrated system theory to achieve their business goals and objectives (Ismail et al., 2014). An assertion relevant to the security framework is that information security relates to the protection of all forms of information and encompasses a broad array of functions both internal and external to an organization (Sindhuja, 2014).

Scholars used integrated system theory as the theoretical framework in security research studies. Dzazali and Zolait (2012), Ismail et al. (2014), Järveläinen (2012), and Sindhuja (2014) used integrated system theory in their information security research studies. Using integrated system theory as a theoretical backdrop, Sindhuja (2014) explored information security initiatives and supply chain performance and operations. Sindhuja (2014) found that information security practices affected supply chain operations of an organization, and that information security practices contributed to managerial planning and strategic decision-making. Sindhuja (2014) also found that by implementing common organizational practices such as training programs, policies, procedures, and well-established communication processes organizational leaders can

solve both technological and cultural challenges found within some organizations. Additionally, Ismail et al. (2014) used integrated system theory in their research relating to the effectiveness of organizational security implementations. In their pilot study, Ismail et al.(2014) found that organizations leaders understood the importance of implementing effective information security controls within critical systems but some leaders failed to establish security training and awareness programs within their organizations.

Using an exploratory approach, Järveläinen (2012) used the integrated system theory and the theory of business continuity management as the theoretical framework in a study of large Finland organizations. Järveläinen (2012) explored the organizational practices that information security and technology leaders used when implementing technology solutions and managing strategic partnerships, outsourcing agreements, or contractual relationships for the procurement of products and services. Using a broad perspective of information technology, security, and business continuity, Järveläinen (2012) found that oversight and governance activities combined with tools such as contract management, auditing, and training enhanced business continuity and information security management within organizations. Similarly, also using an exploratory approach, Dzazali and Zolait (2012) used both integrated system theory and social-technical system theory as the theoretical framework in a study of Malaysia public service organizations. Dzazali and Zolait (2012) examined the factors that may impact the maturity and operations of information security practices within an organization. In their research, Dzazali and Zolait (2012) assessed whether societal aspects such as

organization hierarchies, structures, cultural systems, end user training, and personal factors related to technical aspects of information security. Dzazali and Zolait (2012) found that a positive relationship between an organization's risk management processes and a firm's information security management practices exist. Dzazali and Zolait (2012) findings are consistent with concepts of integrated system theory, and these scholars showed that risk management is a key component of an organization's security framework. Dzazali and Zolait (2012) research also revealed that personal perceptions and awareness about security affected managerial decisions, risk management behaviors, and security implementation these researchers concluded that more positive perceptions of security likely lead to better implementation of security programs within organizations. However, Dzazali and Zolait (2012) research findings are in contrast with the findings of Ismail et al.(2014) where these researchers found that although business leaders of firms may understand the importance of security, some organizational leaders fail to implement appropriate security controls.

Rival and Opposing Theories

In addition to integrated system theory, researchers used other theories and models such as speech act theory, routine activity theory, capability and privacy maturity models, and Crockford's risk-components (CRC) model to examine information security issues and perform research on data breaches (Anandarajan, D'Ovidio, & Jenkins, 2013; Chen, Bose, Leung, & Guo, 2011; Das, Mukhopadhyay, & Anand, 2012; Jenkins, Anandarajan, & D'Ovidio, 2014; Khey & Sainato, 2013; Kwon & Johnson, 2013). Founded in 1962 by Austin, speech act theory relates to the overall comprehensive,

communicative process that individuals use to communicate which includes both spoken language and the intent or implied meaning of messages (Rahman & Gul, 2014). Speech act theory is predicated on the notion that the communication process involves three types of speech acts, *locutionary acts*, actual meaning of words, *illocutionary acts*, the implied meaning of communications, and *perlocutionary acts*, or resulting action, change, or effect on the receiver of the message (Rahimifar & Salim, 2012; Rahman & Gul, 2014).

Speech act theory relates to the manner in which spoken language or written words might affect individual activities, actions, and behaviors (Jenkins et al., 2014), or the resulting effect speech utterances can have on recipients of messages (Mofidi & Shoushtari, 2012). Concepts related to speech act theory include *speech situations, events, and acts* (Nodoushan, 2014). *Speech situations* are the circumstances where speech might occur, such as over dinner or at party, *speech events* relate to the overall behavioral norms and rules governing how speech might occur such as in the classroom or private setting, and *speech acts* refer to the actions, activities, and behaviors, surrounding the speech such as an apology or promise (Nodoushan, 2014). Prior scholars used speech act theory as the theoretical framework of their research when analyzing a variety of textual messages (Fu, 2014). When using speech act theory, scholars evaluate how words, either in verbal or non-verbal form, contribute to individual actions and behaviors (Jenkins et al., 2014). Jenkins et al. (2014) used speech act theory to examine the relationship between data breach characteristics and the structure and composition of breach notification letters published after a security incident and to assess the reputational

effects of organizations affected by data breaches. Jenkins et al. (2014) found that organizations adhered to regulatory requirements and the nature of the data breach incident affected the informational elements organizations included in public notification letters.

Scholars utilized routine activity theory as the theoretical backdrop for information systems security research when assessing the relationship between opportunities or vulnerabilities in an environment and implemented protections and safeguards established within an environment (Khey & Sainato, 2013). In 1979, Larry Cohen and Marcus Felson developed routine activity theory and asserted that the absence of a capable guardian will likely lead to motivated offenders carrying out incidents of crime on suitable victims or targets (Ojedokun, 2012). Proponents of routine activity theory assert that criminal behaviors and activities occur because of individual motivation, suitable victims or targets, and the lack of appropriate guardians and prevention (Anandarajan et al., 2013). Predicated on the notion that everyone has the potential to commit wrongful behavior when given certain opportunities is the basis of routine activity theory (Khey & Sainato, 2013). Proponents of routine activity theory assert that criminal activity will routinely occur if the right circumstances or oportunities exist (Olayemi, 2014) but eliminating or reducing opportunity and implementing appropriate safeguards could minimize or prevent crime (Anandarajan et al., 2013). Researchers can use routine activity theory to understand the motivation of criminal behavior in the technology and security sectors (Anandarajan et al., 2013). Anandarajan et al. (2013) used routine activity theory to examine U.S. data breach notification

reporting laws. Anandarajan et al. (2013) found that there was a significant relationship between the reported number of fraud complaints both before an after the passage of state notification laws. Anandarajan et al. (2013) proposed a generic definition that state officials could adopt in breach notification statutes. Similarly, Khey and Sainato (2013) used routine activity theory as the theoretical basis for their work. Using routine activity theory, Khey and Sainato (2013) examined the spatial and geographic differences among data breaches that occurred within the United States. Khey and Sainato (2013) found that, although data breaches were occurring within large geographic areas, there appeared to be no particular pattern to the types of breach occurrences within the various geographic regions.

In addition to theories, scholars used models when performing information security research (Chen et al., 2011; Das et al., 2012; Kwon & Johnson, 2013). Although origins of the model date back to earlier studies involving organizational quality (Chang, Han, & Chen, 2014), individuals at Carnegie Melon University Software Engineering Institute later developed the capability maturity model (Chang et al., 2014; Filbeck, Swinarski, & Zhao, 2013). The capability maturity model is a framework (Chang et al., 2014) or set of standard principles (Carcary, 2013) that organizational leaders can use to evaluate, understand, assess, and continuously improve operational quality and performance (Carcary, 2013; Chang et al., 2014). Commonly used in the technology industry as a standard model for assessing the quality of software systems and processes, the capability maturity model is a framework that organizational leaders can use to assess the effectiveness of technology services relative to quality, cost, and implementation

timeframe (Filbeck et al., 2013). Included in the capability maturity model are five levels of organizational and operational maturity which range from initial or ad-hoc to optimal (Carcary, 2013; Chang et al., 2014). In a study involving information security, Kwon and Johnson (2013) used the capability maturity model to analyze the relationship between security investments and actual versus perceived compliance. Kwon and Johnson (2013) examined the organizational impact of companies that devoted resources to either preventing security incidents or that later invested in security measures after an event had occurred. Kwon and Johnson (2013) concluded that firms where entity leaders who proactively made a strategic decision to invest in security had fewer data breaches and security incidents resulting in lower costs.

Other scholars used Crockford risk-components (CRC) model in prior research when examining information security issues (Chen et al., 2011; Das et al., 2012). The risk-components model is a risk management model developed by Crockford that includes risks or threats such as natural or human-caused disasters or other deliberate acts of destruction that can disrupt or affect organizational performance (Bose & Leung, 2014). The CRC model is an appropriate theoretical framework that researchers might use to assess how threats of any nature might affect organizational performance (Chen et al., 2011). In their study, Chen et al. (2011) used the CRC model as the theoretical framework to evaluate factors potentially affecting a firm's resources (Chen et al., 2011). The purpose of the study was to understand how breach exposure resulting from phishing incidents potentially negatively impact organizational value in terms of stock price and performance (Chen et al., 2011; Das et al., 2012).

Chen et al. (2011) analyzed the degree to which security breaches caused by phishing attacks and other organizational factors affected the market value of global firms. Phishing is a security threat where unsuspecting individuals are convinced to divulge personal information, which perpetrators can then use to breach or exploit and cause financial or other losses (Chen et al., 2011). From their research, Chen et al. (2011) found that phishing attacks can impact a firm's stock performance. As a result of their research, Chen et al. (2011) developed a new model that entity leaders can use when assessing and estimating the potential severity that a phishing incident could have on a firm's overall value. Das et al. (2012) also used the Crockford's risk-components model to determine the relative impact or effect that data breaches have on the stock price and market value of publicly traded companies. In some instances, Das et al. (2012) concluded that the evidence showed that announcements and public disclosures of data breach incidents could negatively affect a firm's stock market performance.

Risk of Data Breaches

For various reasons such as costs, privacy concerns, potential legal challenges, and other implications, protecting private and sensitive health data is perhaps an issue of increasing importance for some of today's leaders. Private and sensitive information could include clinical records, information about patents, trade secrets, intellectual or proprietary company data, and client records (Chaudhary & Lucas, 2014). Additionally, possible financial implications resulting from security breaches and the frequency of security breaches could contribute to increased awareness of information security issues among top executives (Rajakumar & Shanthi, 2014). Consumers are increasingly taking

legal action against firms due to the rise in the number of recent data breach incidents involving personal information and allegations of theft and identify fraud (Romanosky et al., 2014). The estimated mitigation costs of data breaches in healthcare are greater that the estimated costs associated with mitigation efforts of breach occurrences in other industries (Liu et al., 2015) which could be a concern for business leaders.

Across various industries, information security breach incidents are rapidly on the rise and due to the sensitive nature of medical data and the healthcare industry is not immune from information security threats (Kwon & Johnson, 2014). Data breaches routinely occur and expenses associated with mitigation activities can be costly (Gasch, 2012). Jenkins et al. (2014) noted that data breaches are increasingly commonplace, and the costs associated with breach incidents are normal operational costs of doing business. To highlight the potential magnitude of costs associated with data breaches, Wikina (2014) highlighted that it cost organizations approximately $202 for exposure of a single breached record, and this cost could increase dramatically, depending on the number of records exposed during an incident. Therefore, to reduce the potential impact of information security threats, organizational professionals should retain and store only limited and the minimal amount of information needed to operate their businesses (Rey & Douglass, 2012). Entity leaders who retain more information than necessary to conduct business greatly increase the potential risks and effects of data breaches (Rey & Douglass, 2012). Despite the implementation of strict security measures, vulnerabilities and threats are constantly evolving (Chaudhary & Lucas, 2014). In reality, no single system of information can be totally secure; inevitably data breaches will occur (Arora,

Yttri, & Nilsen, 2014; Chaudhary & Lucas, 2014). Additionally, it appears that no industry is immune or exempt from data breaches (Holtfreter & Harrington, 2015). Security incidents resulting in the exposure of sensitive information occur in almost every major industry such as manufacturing hospitality, financial, telecommunications, including healthcare, non-profit, public sector industries such as governmental, and military (Holtfreter & Harrington, 2015). Healthcare leaders are ultimately responsible for the implementation of appropriate security programs to safeguard, secure, and protect their organizational data (Cucoranu et al., 2013). However, Tu, Spoa-Harty, and Xiao (2015) noted that healthcare entities need effective solutions to minimize the impact of security threats.

Similar to data found in industry sectors such as financial and military, healthcare data contain valuable, sensitive information that attackers may target (Perakslis, 2014). However, in the United States, the HIPAA law contains provisions for organizations to adopt administrative, technical, and electronic measures to help ensure the confidentiality, security, and protection of health-related information (Cucoranu et al., 2013; Rodrigues, de la Torre, Fernández, & López-Coronado, 2013) and other countries have similar rules governing privacy of medical data (Cucoranu et al., 2013). Healthcare data if exposed during a breach can lead to regulatory, reputational, operational, and patient safety risks for organizations (Perakslis, 2014). Vockley (2012) noted that second only to vulnerabilities impacting businesses, the healthcare industry is a prime target vulnerable to data privacy breaches. Perakslis (2014) highlighted that malicious activity taken against medical institutions, clinical practices, and hospitals represented

approximately 72% of attacks while other attacks targeted towards pharmaceutical companies, health plans the other medical facilities represented 28% of attacks.

Information security breaches can affect the stability of critical infrastructure such as power, water, and other systems and lead to economic and financial losses for both customers and businesses (Gordon, Loeb, Lucyshyn, & Zhou, 2015). Data breach incidents can affect and organization's overall security and impact a firm's ability to continue operations (Järveläinen, 2012). In some cases, the impact of information security breaches can have massive implications, drastically affecting an organization's overall security posture, and lead to vulnerabilities and risks, which could jeopardize national security and the public (Wright & Drozdenko, 2013). Van de Meulen (2013) noted that attacks on information security companies, which individuals use to validate the authenticity of internet transactions, possibly signal a growing trend of future attack that could result in both widespread and massive implications. Individuals and businesses depend on, trust, and rely on security products and services, and breaches or exploitation of these products or services could affect critical aspects of the fundamental security infrastructure (van der Meulen, 2013). Thus, due to the potential damage and risks that may occur because of information security breaches, executives and leaders may be shifting their focus and awareness to combating information security threats (Gordon et al., 2015).

In addition to infrastructure threats, unauthorized disclosures and breaches of sensitive information such as personal medical and health data can have tangible and damaging effects for individuals (Hedström, Karlsson, & Kolkowska, 2013). Jenkins et

al. (2014) noted that individuals affected by data breaches are ten times more likely to become victims of identity fraud. Data breaches resulting from unwanted exposure of patient information may affect individual privacy and confidentiality (Ozair, Jamshed, Sharma, & Aggarwal, 2015). Data breaches can affect patient safety as some medical devices used in patient treatment remotely monitor and diagnosis certain medical conditions (Perakslis, 2014). Additionally, security breaches can lead to disruptions of critical infrastructure interfering with or altering critical data and systems that can result in service outages of medical systems and services that patients and individuals depend upon (Perakslis, 2014).

There could be organizational benefits in terms of scalability and cost when deploying advanced technological solutions, but, entity leaders must ensure that private medical information is secured, kept confidential, and protected from unauthorized exposure (Rodrigues et al., 2013). Additionally, the use of automation and mobile computing technologies could enable healthcare organization leaders to gain organizational benefits, regarding costs and operational efficiencies, but advances in mobile automation also increase the risk of vulnerabilities, security incidents, and data breaches (Wirth, 2012). One of the single most important assets of a business is its organizational data or information, but, the unauthorized access, use, or disclosure of sensitive or otherwise protected information can result in unwanted data exposure (Berezina, Cobanoglu, Miller, & Kwansa, 2012). Medical data may contain sensitive records and information such as patient demographical, banking, and other personal data, which make the healthcare industry a likely target for data breaches (Wirth, 2012).

Although there could be positive organizational effects when healthcare leaders implement automation and advanced technologies within their organizations, implementation of these solutions could contribute to consumer concerns regarding the protection, safety, and security of sensitive medical data. Consumer fears could affect advances in healthcare as some individuals may fear the potential effects of data breaches and unwanted exposure of their sensitive information. Additionally, technological advances could lead to opportunities within the healthcare sector, but technological advances may also contribute to uncertainty and consumer concern related to individual privacy, medical error, inappropriate access, or other issues following a data breach (Wirth, 2012). Some researchers noted that consumers might be uncertain, fearful, and concerned about the protection of medical information. Highlighting potential concerns of a data breach, Tu et al. (2015) noted that some consumers are uneasy about the automation of their healthcare data and personal information. As a possible approach of minimizing data loss resulting from data breaches perpetrated by insiders, Tu et al. (2015) proposed an automated approach to monitoring and tracking system-level activities related to employee access to sensitive data stored in healthcare systems.

Similarly, in a study to assess and evaluate the participation and support among healthcare practitioners for health information exchanges, a network of healthcare and medical providers who work collaboratively to provide patient care, Pevnick et al. (2012) noted that some healthcare practitioners were reluctant to join the exchanges. Pevnick et al. (2012) found that one of the major reasons that providers failed to join health information exchanges were fears relating to the potential impacts of data breaches.

Pevnick et al. (2012) found that organizational leaders were reluctant to participate in health exchange networks because of potential public relations, financial, and legal liabilities associated with data breaches.

In terms of protecting private information and safeguarding sensitive medical data, findings of some researchers highlighted that there may be possible reasons, which relate specifically to the healthcare sector, that could contribute to consumer concern, lack of confidence, distrust, and fear (Fernandes et al., 2013; Hedström et al., 2013; Roberts, 2014). Hedström et al. (2013) noted that many of the data breaches occurring at U.S. hospitals commonly related to inappropriate employee access. Roberts (2014) noted that according to data published by the Identity Theft Resource Center, medical entities represented 46 percent of United States data breach incidents that occurred in 2014. Fernandes et al. (2013) conducted a study to determine whether researchers could find personal identifying information such as name date of birth, contact information, medical record number, and other data relating to sensitive patient psychiatric treatment, within an online database that contained masked and obscured electronic medical records. In one instance, Fernandes et al. (2013) found that the database contained identifying information, when aggregated, attackers could use to compromise and expose a patient's medical record. Fernandes et al. (2013) also noted that in some cases, non-sanitized and unobscured patient data existed within the database that perpetrators might access and jeopardize an individual's anonymity.

Data Privacy Breaches and Theft

Data privacy breaches related to theft or accidental exposure could lead to the exposure of medical information. Relative to cybercrime, potential security risks to healthcare data include loss or exposure of information, theft, disruption of medical devices, or downtime of critical infrastructure systems used to support medical services (Perakslis, 2014). Furthermore, theft or unintentional accidents could create risks and lead to the exposure of many patient medical records (Ozair et al., 2015). Cucoranu et al. (2013) noted that during 2009 and 2012, many of the data privacy breach incidents reported to DHHS related to theft or accidental exposure. In 2013, a healthcare employee, working for a university hospital was charged and found guilty of using valid credentials to access, steal, and later sell patient records containing medical record numbers, names, and addresses (Ozair et al., 2015). In another incident, a contractor, who worked for the same hospital, accidentally inappropriately downloaded records onto a laptop, later taken during a theft, contained medical records and personal information of thousands of patients (Ozair et al., 2015). In addition to individual employee actions, accidental release of patient information resulting in data privacy breaches can occur in collaborative research settings (Bredfeldt et al., 2013). During data transfer, Bredfeldt et al. (2013) noted that accidental exposure of patient information can occur when researchers, fail to remove sensitive information such as identification numbers from records, publicly release data meant for local or internal use only, personally communicate about patient personal records, and obtain sensitive information without proper approval or authorization.

Some scholars offered various reasons to explain the underlying cause of breaches and data losses while others scholars noted a linkage between data privacy breaches and theft (Cascardo, 2015; Chen, Ramamurthy, & Wen, 2015; Holtfreter & Harrington, 2015; Tu et al., 2015; Wikina, 2014). In an examination of DHHS breach information, Wikina (2014) noted that causes of data breaches mainly relate to theft and loss. Wikina (2014) found that theft represented approximately 47% of breach incidents and about 27% of breaches related to some form of data loss. Additionally, Cascardo (2015) noted that a significant number of HIPAA violations resulting from data breaches relate to employee theft or unintentional loss. Holtfreter and Harrington (2015) provided a slightly different rationale to describe the three main causes of data breaches and noted that breaches mainly related to inadequate security and disposal of sensitive data, external employee theft, and external hacking or intrusion attempts. However, Chen, Ramamurthy, and Wen (2015) offered a differing view to explain the cause of data breaches. Chen et al. (2015) noted that the source of many organizational data breaches is employee malfeasance or insider threats. Tu et al. (2015) provided an alternative explanation for the cause of data breaches and highlighted that insider theft or espionage are major sources of data loss. Scholarly views regarding the underlying cause of security breaches and opinions on whether external or internal perpetrators commit breach attacks appear mixed. Wright and Drozdenko (2013) noted that the resulting effect of security breaches and attacks perpetrated by insiders far exceed the impact of attacks committed by external hackers or outsiders. However, Holtfreter and Harrington (2015) discovered that outsiders

committed 60% of attacks compared to roughly 40% of breach incidents perpetrated by individuals working within the various organizations.

Other factors may contribute to the underlying cause of data breaches. For example, breaches can occur when perpetrators steal passwords and other information by exploiting vulnerabilities in web applications (Suguna, Kujani, Suganya, & Krishnaveni, 2014). Roberts (2014) noted that a variety of sources can contribute to data breaches that can include external or insider intrusion of attackers, employee accidental or unintentional data loss, insiders who use valid credentials to abuse, exploit, or steal sensitive data for profit, and disgruntled patients and employees who may target certain systems for damage or disruption. Kamoun and Nicho (2014) highlighted that employee malfeasance, negligence, and inappropriate activity caused by excessive system access privileges contributed to data breaches. Data breaches can occur when medical devices that function on pre-packaged commercial software contain software vulnerabilities that attackers can use to exploit interconnected medical network systems (Coronado & Wong, 2014). Security breaches of medical facilities also attributed to device disruptions, system malfunctions as well as data integrity issues (Coronado & Wong, 2014).

Regarding data privacy breaches, the proliferation and use electronic and portable devices can add a level of complexity when it comes to information security (Cascardo, 2015). Illegal activity perpetrated electronic by criminals can have massive implications for both businesses and individuals costing over a billion dollars annually (Roberts, 2014). For example, the theft of stolen medical information can be a valuable revenue source as perpetrators can sell health information on the black market at a premium

(Roberts, 2014). Increased usage of automation technologies and reliance on interconnected, networked solutions in healthcare can contribute to data privacy risks, hacking incidents, promulgation of software viruses, or other issues resulting in system interruptions and malfunctions (Vockley, 2012). Hackers often target medical systems as source of information, which they can then illegally obtain and use to commit fraud as medical data sold on the black market can yield as much as $50 per record (Gray, Citron, & Rinehart, 2013).

Business Associates and Covered Entities in Healthcare

Various medical entities such as hospitals, insurance companies, and organizations are all involved in the protection and management of medical records and health information (Arora et al., 2014).The term entity outlined in different statutes usually mean the type of organization or governmental agency covered under the privacy breach law (Anandarajan et al., 2013). The HIPAA law and Final Privacy Rule govern covered entities, include disclosure rules and protection requirements for health information and outline the appropriate and permissible use of medical data (Goldstein, 2014). However, some medical entities are not considered covered entities and are not subject to HIPAA requirements (Goldstein, 2014). The privacy rules apply only to medical facilities that transmit health information electronically (Goldstein, 2014). Governing provisions of the HIPAA requirements also apply to other organizations and associated providers that electronically transmit protected health data (Flaherty, 2014). In some instances, responsibilities and assurances for the protection of personal health data under the HIPAA Privacy Rule apply to business associates (Wikina, 2014). Healthcare

rules also contain specific security requirements including physical, technological, and administrative provisions applicable to business associates (Clark & Bilimoria, 2013).

Under the HIPAA rules, business associates and covered entities must protect the confidentiality, integrity, and availability of patient medical data and may disclose sensitive health data only under certain conditions (Flaherty, 2014). Medical practitioners should obtain consent to disclose personal health information and should implement appropriate security measures, controls, and safeguards to reasonably secure and maintain the integrity of healthcare systems (Flaherty, 2014). Medical entities and business associates under the HITECH rules must report unauthorized disclosures of medical information and the penalties for violations of the HITECH rules can be severe (Cucoranu et al., 2013). Both business associates and medical service providers could face criminal and civil penalties for inappropriately exposing medical data (Lustgarten, 2015).

Provisions of healthcare laws may apply to medical entities, organizations, and vendors of mobile application solutions. Certain regulatory statutes include provisions for medical organizations to protect personal and financial data (Romanosky et al., 2014). For example, the DHHS maintains and publishes security standards that apply to various medical entities such as health plans, clearinghouses, physicians, and other providers (Lustgarten, 2015). Included in DHHS security standards are provisions that require medical organizations and business associates to safeguard, secure, and protect medical information against data breaches (Lustgarten, 2015). Covered entities must comply with various provisions of the HIPAA rules that include requirements such as implementing

policies and procedures to safeguard electronic medical data and prevent unwanted disclosure of medical information, or these entities can be fined $25,000 to $1.5 million for violations (Cascardo, 2013). Under the HIPAA rules, regulators could fine both business associates and covered entities for compliance violations and failing to protect medical data (Rothstein, 2013). The HITECH and HIPAA laws include mandates for covered entities and medical entities to protect sensitive medical data and including provisions for potential fines and penalties if medical practitioners breach patient information (Rey & Douglass, 2012). Included in the HITECH rules are security standards, provisions, and legal liabilities for medical service providers such as health plans and clearinghouses to protect and secure private health information (Lustgarten, 2015). Additionally, mobile applications that store medical and personal health data deployed within some medical entities must adhere to certain HIPAA security standards (Flaherty, 2014).

However, despite potential legal consequences and regulatory requirements to protect medical data, unwanted exposures of private health information through various means may still occur. Unwanted exposures of information and data breaches mainly include inappropriate handling, destruction, or disposal of data, theft of computing devices containing sensitive records, or unauthorized attempts to gain access to computing systems via hacking (Romanosky et al., 2014). External vendors, third party associates, and outsourced partners can contribute to data breaches, which may damage a firm's reputation and affect the organization's overall strategic value (Järveläinen, 2012). Third party vendors and business associates can expose patient information representing

a rapidly growing source and major cause of data breaches (Wilkes, 2014). Sources of data breaches include system malfunctions and inappropriate activities of third parties (Berezina et al., 2012). Willey and White (2013) noted that in 2011, external agents or otherwise third party business associates represented 98% of breach incidents. In a study to determine the types and characteristics of breach incidents, Liu et al. (2015) found that issues caused by business associates or external third-party vendors represented 28 percent of all reported breach cases examined.

Record Exposure and Location of Breach Information

Data breach exposures could include a wide array of information, documents, and records. Individual personal health information may exist in various forms including both paper and electronic records (Rey & Douglass, 2012). Although confidential information may exist in various forms, confidential and sensitive personal information is a valuable asset that organizations must protect (Taylor & Robinson, 2015). Various laws and regulations include provisions that organizations must prevent unwanted disclosure of information and protect sensitive information from data breaches (Tu et al., 2015). Once processed private and sensitive information may be stored and maintained in various media including paper documents, compact discs, backup tapes, or other electronic means (Taylor & Robinson, 2015).

Information stored in a variety of formats could if not appropriately secured can result in the exposure of sensitive information. Often, healthcare practitioners generate, maintain, store, and destroy personal health data during various phases of the medical process that may need certain security protections (Rey & Douglass, 2012). There could

also be potential drawbacks resulting in unwanted data exposure associated with storing data in various forms such as paper, physical, or electronic means (Lustgarten, 2015). Risks to physical and paper records include theft and damage caused by disasters, and with electronic records, there could be concerns about unwanted access (Lustgarten, 2015). Various sources including individuals, businesses, and governmental agencies may store sensitive or personal information that attackers could exploit, expose, steal, or use to commit different types of fraud (van der Meulen, 2013). For example, in a review of DHHS data breaches, Wikina (2014) found that for individuals, the source of breached records mainly included data stored on removal media, desktop computers, and other electronic devices, yet the source of breach incidents for covered entities and business associates were physical documents, portable electronic devices such as laptops, and removal media.

Data breaches could lead to unwanted exposure or data loss of records containing sensitive information. Anandarajan et al. (2013) noted that from 2004 to 2009 a report published on behalf of the United States Secret Service showed that data breaches exposed 912,902,402 records. Layton and Watters (2014) noted that in 2012, a social networking firm, exposed over 6.4 million password hashes, and potential attackers could use the breached information to determine the actual passwords of customers. Highlighting the potential exposure of data breaches, Silverman (2014) noted that in 2013, data losses occurred in approximately 1,367 of the nearly 63,000 worldwide reported cases of security incidents. From 2005 to 2010, Anandarajan et al. (2013) noted that a report from the Digital Forensics Association Widup showed that were 806.2

billion records exposed in data breach incidents. Anandarajan et al. (2013) also reported that there were nearly 419 privacy breaches, in 2011 that resulted in sensitive data exposure for over 21 million people.

Unauthorized disclosures and data breaches may include an array of sensitive information. During a data breach in 2012, a data breach of a U.S. based online shoe retailer disclosed over 24 million scrambled passwords, portions of credit card numbers, including certain identifying customer information. Also in 2012, a security incident occurring when a high level employee working for the South Carolina Department of Revenue, opened an email attachment sent from an unknown source, resulted in the exposure and theft of confidential information of 3.8 million taxpayers, over 3 million bank account numbers, and tax information of 699,900 businesses (Loy, Brown, & Tabibzadeh, 2014). In 2013, external attackers during a theft incident accessed records of a large retailer which led to the exposure of credit cardholder data of roughly 40 million customers (Chaudhary & Lucas, 2014). During the breach, attackers also gained access to other sensitive information including telephone numbers and address information of nearly 70 million individuals (Chaudhary & Lucas, 2014).

Breach incidents may also include the exposure of personal medical records or result in penalties for improper exposure of medical data. Each year data breaches occur, leading to the exposure of millions of patient records containing sensitive information such as name, social security number, insurance claim and medical numbers, birth and address information, financial data, and personal health records such as medical treatment and diagnosis information (Vockley, 2012). However, the actual occurrence and number

of data breaches incidents are relatively unknown because some organizational leaders fail to report or disclose data breaches (Roberts, 2014). In some cases, entity representatives may be unaware that a breach incident even occurred (Roberts, 2014). In 2012, a breach launched by external hackers against a Utah-based healthcare facility led to the exposure of roughly 780,000 patient medical records (Gray et al., 2013). During the Utah breach, attackers were able to obtain personal patient information that included social security number and medical diagnosis codes which they could use commit medical fraud (Gray et al., 2013). In 2013, a Florida healthcare system exposed over 1,000 patient records during a data breach (Wikina, 2014). A breach involving data services containing health information lead to the loss of 1.9 million patient records (Vockley, 2012). Additionally, a breach incident resulting from a software update made to website affected 1,350 surgery patients of a California healthcare system (Wikina, 2014). A breach consisting of both financial and medical information stored on backup tapes, stolen during a car break-in belonging to an employee of a healthcare institution, resulted in a $4.9 billion class action lawsuit and the unwanted exposure of 5.2 million patient records (Vockley, 2012). In another incident, a data breach of a California-based medical institution resulted in the filing of two class action cases and the exposure of 4.2 unencrypted patient records. In 2013, officials of the OCR imposed fines more than roughly $900,000 when a medical facility for failing to implement adequate security measures (Chaudhary & Lucas, 2014). Leaders of a managed care facility, in 2013, settled with OCR for $1.7 million for security violations under the HIPAA Privacy Rules (Chaudhary & Lucas, 2014).

From time to time, researchers also highlighted that data breaches can result in the unwanted exposure or disclosure of sensitive patient medical records (Gasch, 2012; Hayhurst, 2014; Kwon & Johnson, 2013). Hayhurst (2014) highlighted that data breaches might potentially affect personal medical records. Kwon and Johnson (2013) noted that within the first two years of collecting information on data breaches, DHHS officials reported that healthcare organizations disclosed approximately 10 million records containing sensitive patient data despite substantial improvements and advancements in security. Similarly, Gasch (2012) noted that since the passage of the HITECH law, data breach exposure of roughly 385 information security incidents affected approximately 19 million patient records. Hayhurst (2014) highlighted that data privacy breach incidents of healthcare entities, reported to DHHS, involving breaches of 500 or more records affected over 29.2 million patient records. Hayhurst (2014) noted that in 2013, data breaches affected approximately 7.1 million records with a single breach incident affecting over 4 million patient records. Researchers (Gasch, 2012; Hayhurst, 2014; Kwon & Johnson, 2013) all seemed to highlight the importance of understanding information security issues and how these issues might relate to data breaches of sensitive medical records.

Possible Effects of Data Breaches

Organizational leaders increasingly rely on information systems to operate their businesses, but, individuals can expose information that resides within these systems resulting in unwanted exposures, losses, and data breaches (Chang & Wang, 2011). For example, a significant number of healthcare practitioners routinely use electronic devices

and smartphones (Wirth, 2012). Medical personnel now have access to many applications via their mobile phones and other electronic devices that they can use to facilitate and manage patient care (Wirth, 2012). Providers can now perform functions such as processing prescriptions and updating patient medical records via a mobile device or computer (Schulke, 2013). However, a changing technological logical landscape could lead to increasing data privacy challenges, vulnerabilities, and difficulties for medical providers responsible for protecting sensitive client data (Lustgarten, 2015). Data breach incidents could affect an organization and impact an entity's ability to continue operations (Järveläinen, 2012).

Data breach and security incidents can affect patient health and safety and have organizational and individual effects. For consumers, unwanted disclosures and breaches of personal and sensitive data can contribute to medical, financial, and identity fraud (Romanosky et al., 2014). Security incidents and breaches could affect the quality of patient care and individual health safety (Vockley, 2012). Breaches and attacks on health systems can affect vital patient services such as portable individual implantable devices and insulin pumps, or affect other business related medical services (Vockley, 2012). Data security breaches can render healthcare systems offline or contribute to prolonged service disruptions (Vockley, 2012). Security incidents can lead to delays in patient treatment, reduce staff productivity, and have financial implications for healthcare organizations if systems are offline for prolonged periods of maintenance or repair (Vockley, 2012). Roberts (2014) indicated that due to data breaches, health related dangers could include wrongful modification, tampering, or merging of personal medical

information with other medical records. Physicians might erroneously use information found in breached records that could lead to improper diagnosis, treatment, or other implications, and in some cases can affect a person's overall health or contribute to a patient's death (Roberts, 2014).

Data breaches may have a variety of individual and organizational effects. Roberts (2014) indicated that breaches of healthcare data have three main effects financial, health, and reputational. Data breaches can also have an organizational effect on firms in terms of mitigation, investigative, and response costs (Telang, 2015). Abu-Musa (2010) conducted a survey of Saudi organizations and found that security breach incidents affected over half of the organizations, but the actual cost associated with the damages relating to the breach were unknown. Gatzlaff and McCullough (2012) also noted that security incidents could lead to decreases in stock price, reputational effects, and exposure of trade secrets or other sensitive information. Although it is difficult to determine the actual costs of data breaches, effects of data breaches might include unwanted costs of fines and penalties, expenses to cover the costs of system security upgrades, legal costs related to challenges brought on by stakeholders, and payments for reimbursement of fraudulent charges (Gatzlaff & McCullough, 2012). There are both direct costs and indirect costs associated with data breaches (Layton & Watters, 2014). Direct costs include expenses associated with investigative, staffing, compliance, legal, notification, mitigation, interests, and borrowing (Layton & Watters, 2014). Indirect costs relate to the loss or reduction in potential revenues, negative effects on reputation, image, brand, operational disruptions, employee burnout, or loss of staff productivity (Layton &

Watters, 2014). Data breaches might also lead to outages, system downtime, service interruptions, and loss of consumer confidence and loyalty (Gatzlaff & McCullough, 2012).

In addition to organizational effects, there could be some potential personal effects of data breaches. Data breaches may affect consumers leading to various forms of medical or financial fraud (Telang, 2015). In some instances, individuals may not even fully recover from all damages suffered during the breach (Telang, 2015). According to Roberts (2014), data breaches could lead to fraudulent medical claims and services or the exposure of certain illnesses or conditions in a patient's medical history could have individual impacts. For example, exposure of medical information could damage potential employment or have other societal effects (Roberts, 2014). Jenkins et al. (2014) noted that in 2011, there was a 67% increase in the number of data breach incidents, which affected millions of Americans, compared to the number of breach incidents in the prior year. Other potential personal effects of data breaches might include identity fraud, loss of earnings, and costs for additional protections for credit monitoring and insurance (Gatzlaff & McCullough, 2012). Holtfreter and Harrington (2015) noted that according to the Federal Trade Commission (FTC) there are approximately 10 million reported cases of identity theft annually in the U. S. but the actual number of cases could be higher as some individuals never disclose or report identity theft cases.

Prior Research on Data Breaches

In the past, analysis of data breach and security threats consisted of an array of research approaches and methodologies. Using secondary data collected from multiple

sources, Sen and Borle (2015) used a quantitative research approach when analyzing the impact of publicly disclosed data breaches and vulnerabilities of organizations. Sen and Borle (2015) examined the risk to certain industries based upon the types of breach incidents and analyzed the occurrences of breach incidents within various states. Sen and Borle (2015) found that the passage of strict laws and regulations had no effect on the risk of occurrence of data breaches at the state level. In terms of adoption of stricter laws and the relative effect on breach incidents, Sen and Borle (2015) discovered that the risk of data breaches decreased in certain industries such as healthcare and nongovernmental organizations, but the passage of strict legislation had only a minimal effect on other industries such as education, governmental, retail, and insurance. Sen and Borle (2015) research also revealed that data breaches contributed to loss or theft occurred more frequently than breaches related to malicious intent.

Sen and Borle (2015) also showed that stronger legislative laws also appeared to reduce the number of privacy breach incidents involving leakage or exposure of sensitive or personal information. Furthermore, Sen and Borle (2015) in their work also found that investments in security did not decrease the risk of data breaches. The findings of Sen and Borle (2015) are somewhat different from earlier findings on the effects of security investments and security incidents. Earlier studies on security investments by Kwon and Johnson (2013) showed that for mature hospitals, investments in technological security resources and implementing preventative practices had a casual effect on data breaches resulting in fewer breaches. Examining secondary data collected from a hospital survey, Kwon and Johnson (2014) used a quantitative research approach to examine the effects of

security investments on data security incidents and failures. Kwon and Johnson (2014) found an association between proactive versus reactive resource investments and a reduction in the number of data security incidents of firms.

Similarly, using secondary data to perform a quantitative study, Kwon and Johnson (2013) analyzed secondary data provided by hospital technology managers who completed a survey questionnaire that included both open and closed questions. In their study, Kwon and Johnson (2013) assessed the impact of security investments and resources on actual and perceived compliance. Kwon and Johnson (2013) found that depending on the operational maturity of the hospital security investments could have either a significant or minimal effect on an institution's overall level of compliance. In terms of prevention, Kwon and Johnson (2013) discovered that investments in security resources appeared to have a significant effect on compliance when organizations are more mature and when leaders effectively allocate resources between both prevention and data security efforts. Evaluating the characteristics and scope of healthcare data breaches, Liu et al. (2015) conducted a quantitative study using secondary data retrieved from DHHS's online breach reports. Liu et al. (2015) found that data breaches occurred in all U. S. states as well as Puerto Rico and the District of Columbia and five states California, Texas, Florida, New York, and Illinois represented over a third of the total number of reported breach incidents. Liu et al. (2015) determined that a significant portion of healthcare data breaches involved information residing on electronic media such as portable computing hardware, incidents relating to theft, or stolen records. Liu et al. (2015) also noted that there was an increase in the number security incidents involving

hacking. Furthermore, there was a rise in the number of incidents related to improper access and disclosure of sensitive information (Liu et al., 2015). Liu et al. (2015) determined that criminal behavior was the underlying cause of most data breaches.

In addition to Kwon and Johnson (2013), other scholars (Holtfreter & Harrington, 2015; Romanosky et al., 2014) used secondary data sources in quantitative research studies related to data breaches. Romanosky et al. (2014) investigated the types, reasons, and characteristics of federal lawsuits involving data breaches and assessed the resulting outcomes of breach litigation. Romanosky et al. (2014) found that individuals are 3.5 times more likely to sue when individuals experience financial or medical fraud resulting from a data breach. Plaintiffs also tend to sue if the breach incident relates to improperly discarded information and are six times more likely to initiate a lawsuit when the incident involves data loss or theft of financial data (Romanosky et al., 2014). Romanosky et al. (2014) discovered that breach cases are ten times more likely to end in a settlement when the breach incident related to a cyber-attack, theft, or loss of hardware. Companies leaders are also 30 percent more likely to settle a case if there is a potential that the case merits are worthy of a certified class action lawsuit status (Romanosky et al., 2014). Finally, data breach incidents involving medical data could pose financial risks to medical entities, Romanosky et al. (2014) determined that breach cases relating to the exposure of sensitive medical information are 31 percent more likely than other cases to result in settlement. Scholars conducted other data breach research using quantitative approaches. In a quantitative study using secondary data obtained from the Privacy Rights Clearinghouse, Holtfreter and Harrington (2015) examined data breach trends in

the United States. Holtfreter and Harrington (2015) sub-divided data breaches into non-traceable, external, or internal categories depending on whether the occurrence of the breach incident was traceable and attributed to internal or external perpetrators. Holtfreter and Harrington (2015) also examined breach patterns across various industries. Based on their findings, Holtfreter and Harrington (2015) determined that, regarding records compromised, there were more breach incidents perpetrated by external attackers compared to the number of breach incidents committed by insiders. Holtfreter and Harrington (2015) discovered that external threats and outsiders caused 60% of breaches compared to roughly 40% of breach incidents perpetrated by insiders or employees of the organization. Holtfreter and Harrington (2015) also found that breaches occur in all industries and breaches could result in the unwanted expose of millions of records. Holtfreter and Harrington (2015) noted that data breaches relate to three main causes, which include failing to secure and appropriately dispose of sensitive data, theft, or malfeasance committed by non-employees, and external hacking or intrusion attempts.

Researchers Chen et al. (2012) also used secondary data in a quantitative study to examine data breaches. Using secondary data obtained from the web site attrition.org, Chen et al. (2012) analyzed whether data breaches that occurred at clients of technology consulting firms had adverse effects on the share price of the North American consulting firms. The overall goal of Chen et al. (2012) study was to assessed whether breaches of prior clients, sites where the employees of the technology consulting firm implemented the breached technology or system, might affect the future value or earnings technologyof the consulting firm. Chen et al. (2012) found that overall client data

breaches only had an immediate negative effect on stock prices of technology firms. However, Chen et al. (2012) discovered that when client breaches involved a significant number of breached records, there were negative effects on the firm's stock price. Chen et al. (2012) also noted that breaches had an even greater impact on stock price and profitability when prior clients of the consulting firm operated in either the technology or retail industries.

Scholars utilized qualitative approaches when conducting security research on data breaches (Adebayo, 2012; Jenkins et al., 2014; Kamoun & Nicho, 2014). Using a qualitative research approach, Adebayo (2012) evaluated public repositories containing published information about data breaches that scholars often use in data breach research. Adebayo (2012) determined that no single repository contained comprehensive information about all breach incidents. Adebayo (2012) concluded that using a combination of online data repositories supplemented by independent verification of breach information might be an effective approach that researchers can use to gather information when conducting research relating to data breaches. Jenkins et al. (2014) used qualitative content analysis to evaluate the composition of breach notification letters crafted in response to breach incidents. In their study, Jenkins et al. (2014) also performed an experiment in which the researchers analyzed consumer perceptions of notification letters and other communication messages related to breach incidents on an organization's reputation. Jenkins et al. (2014) determined that correspondence relating to breach incidents often contained limited information about the security incident. However, Jenkins et al. (2014) found that notification correspondence relating to breach

incidents included statements about the organizational importance and seriousness of the incident (Jenkins et al., 2014). Based on the results of the study, Jenkins et al. (2014) found that statements of empathy and apology can have positive reputational effects. Using a combination of online data sources, which consisted of information derived the Open Security Foundation, United States DHHS's online breach database, Privacy Rights Clearinghouse, and Big Brother Watch, Kamoun and Nicho (2014) used a qualitative approach to analyze the human and organizational factors and underlying root causes of data breaches. Based on their analysis of prior breaches, Kamoun and Nicho (2014) proposed a theoretical model consisting of organizational factors, inadequate security defense mechanisms, improper data handling practices, and lack of effective communication and organizational strategies led to the precursors of mismanagement and are contributory factors underlying the cause of data breaches. Kamoun and Nicho (2014) noted that healthcare leaders should adopt a defense-in-depth strategy that consists of implementing a combination of technical, physical, human and other measures to prevent data breaches. Kamoun and Nicho (2014) research results revealed that a combination of human errors, lack of appropriately designed technical systems, and inadequate governance, societal, and organizational systems contributed to breach incidents.

Layton and Watters (2014), similar to other scholars Adebayo (2012), Kamoun and Nicho (2014) and Jenkins et al. (2014), used a qualitative approach in their research of data breaches. Using a cost estimation model, Layton and Watters (2014) analyzed two case studies and evaluated the overall costs to organizations, both tangible and intangible, associated with data breaches. Layton and Watters (2014) found that an analysis of both

firms revealed that the stock price of firms increased following the data breach. Therefore, Layton and Watters (2014) determined that indirect or intangible costs such as loss of reputation, corporate image, and customer loyalty did not have a significant impact on organizational value (Layton & Watters, 2014). Scholars Layton and Watters (2014) also discovered that organizational and business practices could lower the overall resulting costs of data breaches. However, Layton and Watters (2014) also found that direct costs associated with breaches can be quite expensive and, therefore, noted that business leaders should consider investing in security and prevention activities.

Transition and Summary

Section 1 included an overview and introduction of the proposed study on data breaches within the healthcare sector. Also presented in Section 1 was information regarding the background, significance, and the relative importance of data breach research to medical practitioners and technology professionals. The literature review presented in Section 1 contained information about potential societal and organizational outcomes that might occur when custodians of medical or health related information fail to secure health information and adequately protect sensitive data. Information presented in the literature review validated and highlighted the need for the study, which could provide business leaders with knowledge and insights about the significance of security prevention and possible effects that data breaches can have on organizational value.

The overall goal of Section 2 is to provide readers with an understanding of the research plan. In Section 2, I include an overview of the research project and proposed plan for the study. I outline the overall nature of the study, population, data collection,

and analysis procedures, and provide justification for the chosen research methodology and design. In section 2, I also discuss concepts of ethical research and explain how I ensured scientific rigor when conducting the study.

Section 2: The Project

In this section, I present the overall goal of the study and detail the proposed research plan. A discussion of the research project follows, and I explain various research methods and design approaches as well as highlight key methodological and design considerations. Also included in this section is an explanation of appropriate statistical and data analytical procedures chosen for this study. I also discuss the proposed data collection processes for the study and describe the steps that I performed to help ensure that research conclusions and observations are scientifically sound, valid, and reliable.

Purpose Statement

The purpose of this quantitative loglinear study was to examine the association between data privacy breaches, business associates, covered entities, the number of individuals affected, and data storage locations. The variables were data privacy breaches, covered entity types, number of individuals affected, storage location of breach data, and business associates. The study took place in Atlanta, Georgia, and the population included secondary data related to breach incidents reported by healthcare leaders across the United States in years 2009 to 2016. Findings from this research could provide healthcare practitioners and other business professionals with knowledge, information, and understanding of relationships associated with data privacy breaches. Healthcare leaders might use information from this study to change business practices, implement appropriate preventative measures, and manage data security effectively. Contributions to social change might include healthcare practitioners utilizing the findings and recommendations from this study to improve and better secure private

medical records of patients and individuals. Another contribution to social change might include healthcare leaders utilizing the findings presented in this study to minimize data security risk factors, protect sensitive healthcare data, and reduce costs associated with breach mitigation and response activities.

Role of the Researcher

In scientific inquiry, the researcher is the data collection instrument and conduit for information flow (Whiteley, 2012). The researcher is the primary individual who collects data, interprets information, and makes sense of results (Tomkinson, 2015). Researchers manage the research setting, engage participants, report information, and choose pertinent data to report (Tomkinson, 2015). A researcher's main role in the research process is interpretive, providing thorough and rich explanations or meanings about data or phenomenon (Lalor et al., 2013). In search of understanding and obtaining knowledge, researchers highlight and explain the views and ideas of others (Paull, Boudville, & Sitlington, 2013). Although essential to the study, researchers should understand that they conduct their work through a personal perspective poosibly influenced by individual biases, cultural experiences (Fusch & Ness, 2015), specific values or belief systems, and worldviews (Zohrabi, 2013). Researcher bias can occur during various phases of the scientific discovery process and might affect interpretations of results (Peterson et al., 2015). During data collection, researchers should take steps to mitigate bias and ensure that personal biases do not adversely affect their work (Fusch & Ness, 2015). When performing their work, researchers should strive to be as objective, honest, and explicit in their approach as possible (Zohrabi, 2013). Thus, scholars must

have a persistent awareness of how knowledge differences in certain areas may affect their work (Bulpitt & Martin, 2010).

Authors must disclose and highlight any potential sources of conflicts including any relationships, financial conflicts, affiliations, or other actions or activities that may exist in their work that could affect research outcomes (Masic, 2012). In this regard, I disclose prior work experience, training, and formal education relating to the field of information systems security. I also hold a certified information systems security (CISSP) professional industry certification issued by the International System Security Consortium Incorporated. However, my prior information security work experience has not specifically been in the healthcare sector. Therefore, my prior knowledge, work experience, training, and professional expertise did not bias or negatively influence my research in any way.

Developed in 1979 by a commission of the U. S. government, the Belmont Report contains information regarding certain protections and guidelines for human subjects research and includes research considerations for vulnerable individuals, populations, or groups (Rogers & Lange, 2013). Outlined in the Belmont report is information about ethical guidelines, research principles, and considerations researchers should be aware of when performing their work (Rogers & Lange, 2013). I followed the guidelines and principles outlined in the Belmont Report. Prior to commencing the study, I obtained explicit permission from Walden University's Institutional Review Board, approval number 03-18-16-0077321, to utilize information contained in the online database for research.

Behavioral guidelines, professional standards of conduct, and oversight committees exist, but ultimately researchers select the value system and moral code they use in their research (Fouka & Mantzorou, 2011). During the research process, I behaved ethically, adopted high standards of moral conduct, and maintained a constant awareness of how my professional expertise and knowledge differences might have affected my work. Governing principles of scientific inquiry are community, beliefs, social norms, and ethical issues that relate to situations or actions involving right and wrong (Fouka & Mantzorou, 2011). A relationship of trust is the foundation for scientific inquiry and ethical mishaps or judgmental lapses by researchers can damage humans, animals, and the public (Gomes, Saha, Datta, & Gomes, 2013). Ethical misconduct is any falsification, misrepresentation, or fabrication of data, information, or outcomes involved in the research process (Gomes et al., 2013).

Ethics, developed from the Greek term ethos for custom or character, relates to the actions, decision making processes, understanding of situational conflicts, and behavioral choices of researchers (Avasthi, Ghosh, Sarkar, & Grover, 2013). Although activities involving scientific inquiry might affect participants or personally affect researchers in some manner, scholars must behave honestly and conduct their work in an ethically sound manner (Pesonen, Remes, & Isola, 2011). Researchers could influence the outcome of their studies (Bulpitt & Martin, 2010). Therefore, scholars must conduct their work in an open, transparent, trustworthy, and credible manner (Bulpitt & Martin, 2010). To ensure the credibility of my work, I conducted my work in an open, honest, trustworthy, and transparent manner.

Participants

In the study, I collected and analyzed information available from a secondary data source, and I did not collect information directly from individual participants. The data source that I used for the study is publicly accessible and available online from the U.S. Department of Health & Human Services Office for Civil Rights (OCR). Under the HIPAA law, representatives of the OCR handle and oversee the enforcement of certain protections granted to individuals regarding their personal medical information (Cascardo, 2012; Wikina, 2014). The data that officials of OCR collect is not subject to disclosure restrictions, special handling, or data retention requirements as this information is already in the public domain. Using the OCR online data source, I reviewed information about privacy breaches of healthcare data reported during years 2009 through early 2016. Therefore, the participants section is not applicable to this study, as I did not use any data that I derived or collected from individual participants.

Research Method and Design

Scholars often categorize research methodologies as either quantitative, qualitative, or mixed (Long, 2014). The research method is the overarching process or logical flow and the theoretical basis from which scholars approach the study (Long, 2014). Research methods are the tools, techniques, and procedures researchers use when evaluating and analyzing the data gathered during the study (Long, 2014). Measurement, experiment, and statistical analysis are techniques quantitative researchers often utilize in their work (Long, 2014). Techniques commonly used by qualitative researchers are observation, interviews, and content analysis (Long, 2014). The research methodology

that I selected for this study is the quantitative method, and I used techniques and procedures appropriate for a loglinear analysis design.

Method

Quantitative scholars tend to believe that through objective and tangible means such as statistical analysis and measurement, they can uncover information about existing relationships among variables and factors that naturally exist (Long, 2014). Using measurement indicators in a controlled setting, quantitative researchers seek understanding of a phenomenon (Masue, Swai, & Anasel, 2013). In quantitative research, data is collected, interpreted, and represented numerically (Yoshikawa, Weisner, Kalil, & Way, 2013). Quantitative researchers use statistical tools and attempt to analyze various data elements to accurately describe, summarize, and depict characteristics of individuals, situations, or groups (Ingham-Broomfield, 2014). The overall goal of quantitative research is to test hypotheses (Morgan, 2015). Extending from a hypothesis and through an objective measurement process, quantitative researchers use statistical tools to investigate and explain data and facts using numbers (Arghode, 2012). Similarly, in this study, I used quantitative techniques to test hypotheses, used statistical tools to investigate and explain data, and presented test results numerically.

Conversely, qualitative researchers hold the view that the knowledge process is more subjective in nature, and they attempt to decode, translate, and interpret the meaning of data through various social interactions such as interviews and observations (Long, 2014). When performing qualitative research, scientists often choose designs such as phenomenology, grounded theory, ethnographies, case studies, or focus groups

(Holosko et al., 2014). Qualitative researchers attempt to explain and describe phenomenon by identifying similarities and themes rather than manipulating variables (Holosko et al., 2014). In a more natural setting, such as interviews and observations, qualitative researchers explore a particular phenomenon to uncover multiple perceived meanings of data (Arghode, 2012). Data collected non-numerically via text, narrative descriptions, and observations are representative of qualitative research (Yoshikawa et al., 2013).

Scientists systematically combine aspects of both quantitative and qualitative approaches into a single integrated comprehensive review (Heyvaert, Maes, & Onghena, 2013). In mixed method research, scholars tend to believe that combining both qualitative and quantitative methodological approaches somehow validates the legitimacy of the study (Long, 2014) and enables researchers to gain a deeper and more complete understanding of the various meaning of the data (Yoshikawa et al., 2013). Mixed method researchers combine aspects of both qualitative and quantitative research into a single study (Long, 2014; Siddiqui & Fitzgerald, 2014).

The goal of this study was to examine variables and perform hypothesis testing using a nonexperimental design approach. In this study, I did not use various social interactions, and I did not decode or interpret information non-numerically. For this study, I also did not combine aspects of the qualitative and quantitative research approach. Therefore, neither a mixed nor qualitative research method was appropriate for this study. Alternatively, through statistical analysis and numbers, I uncovered

information about relationships that may naturally exist and thus the quantitative method was appropriate for this study.

Research Design

In scientific research, there are numerous qualitative and quantitative research design approaches (Yoshikawa et al., 2013). Within quantitative research, there are various design approaches such as survey research, systematic reviews, experimental, quasi-experimental, nonexperimental, correlational, and casual-comparative studies that researchers can choose to perform (Turner, Balmer, & Coverdale, 2013). Utilizing a nonmanipulative design approach, researchers use correlational designs to identify, clarify, or describe the relationship between variables (Holosko et al., 2014; Turner et al., 2013). The research design selected for this study was a quantitative loglinear analysis research approach.

Developed in the 1970s by Goodman as an alternative to independence models, loglinear models are effective statistical means to analyze categorical data (Sloane & Morgan, 1996). When analyzing relationships and interactions among multiple response variables, a researcher may use loglinear procedures (Onder, Onder, & Mutlu, 2012). A loglinear design approach is appropriate when understanding the relationships between multiple categorical variables (Mettke-Hofmann et al., 2015; Olmuş & Erbaş, 2012; Vaid, 2012) and when examining the interactions (Din, Zugman, & Khashper, 2014; Olmuş & Erbaş, 2012), inter-relationships, and associations among variables (Olmuş & Erbaş, 2012). The variables included in the dataset that I analyzed for this study were categorical in nature. Loglinear models are appropriate for variable interactions of three-

factor and beyond (White, Tansey, Smith, & Barnett, 1993). Thus, quantitative loglinear designs are useful in determining the relational significance, magnitude, and direction among categorical variables (Haque, Chin, & Debnath, 2012).

The overall goal of quantitative research is to determine the relationships between one or more variables (Bettany-Saltikov & Whittaker, 2014). Quantitative scientists examine variables using statistical or numerical means (Holosko et al., 2014) and may utilize a nonexperimental or experimental research design (Birchall, 2014). Within quantitative designs, there is descriptive research, a form of survey research, where researchers use surveys to determine and describe the characteristics and specific details of a population (Turner et al., 2013). I did not utilize surveys to determine and describe the characteristics and specific details of a population. Thus, a quantitative descriptive design was not appropriate for this study. In quasi-experimental research designs, an investigator manipulates an independent variable, but with these designs control is somewhat limited because subjects cannot be randomized (Ingham-Broomfield, 2014). In quantitative experimental designs, researchers systematically and objectively control independent variables and assign subjects to different conditions (Ingham-Broomfield, 2014; Welford, Murphy, & Casey, 2012). The goal of this study was not to manipulate variables and assign individuals to different conditions thus neither a quasi-experimental design or experimental design was appropriate for this study.

Population and Sampling

The overall population for this study consisted of U.S. medical organizations covered under the HIPAA law that store, transmits, or manage protected health

information. Requirements under the HITECH law include provisions for covered entities to report data security incidents that may involve potential inappropriate disclosures of personal health information (Coronado & Wong, 2014). For security incidents that involve at least 500 individuals, the HITECH law specifically mandates that DHHS officials disclose and post online via web notification templates, information about breach cases that DHHS investigates and resolves (Liu et al., 2015). In 2010, OCR first publicized information regarding breaches of unsecured health data (Cascardo, 2012). For this study, I used the OCR breach database. Wikina (2014) also used information from DHHS's publicly available website to analyze healthcare breaches trends.

Researchers should carefully choose appropriate sampling techniques in their studies thereby saving valuable time, money, and resources (Shorten & Moorley, 2014). Two main sampling methods are non-probability and probability sampling (Kandola, Banner, O'Keefe-McCarthy, & Jassal, 2014). Probability designs usually consist of one of five main types of sampling known as *simple random*, *systematic*, *stratified*, *cluster*, and *multi-stage* sampling (Kandola et al., 2014). Probability sampling, often found in quantitative research, involves randomly selecting equal and independents elements from a population (Kandola et al., 2014). When researchers need to ensure representation of the population and increase the level of robustness and precision of the study probabilistic selection procedures are more appropriate (Espinosa, Bieski, & Martins, 2012).

Advantages of probability or representative sampling techniques are that researchers eliminate bias, and all elements of the population have an equal chance of

random selection (Shorten & Moorley, 2014). Minimizing researcher bias and reducing the likelihood of skewed results are other advantages of probabilistic designs (Kandola et al., 2014). Disadvantages of probabilistic designs include cost and time; however, using technological advances researchers can manage disadvantages (Baker et al., 2013). Although not the single or most commonly used method of forming statistical inferences, in certain forms of research, probability sampling is often a standard inferential statistical research approach (Baker et al., 2013). An ideal sampling method for this study could be a probabilistic sampling approach. However, for this study, I did not sample a select number of records for review. Conversely, I examined and analyzed information relating to all privacy breach incidents affecting 500 or more individuals reported to DHHS and resolved by OCR officials since the passage of the HITECH law in 2009 through early 2016.

In their studies, quantitative researchers perform a power analysis to determine the appropriate sample size required for detecting and determining a statistically significant difference or result that can affect the reliability of conclusions (Tomczak, Tomczak, Kleka, & Lew, 2014). Several factors affect the power of a study including effect size, variability of the data, and predetermined level of significance (Tomczak et al., 2014). Some researchers noted that a power analysis is not needed or appropriate in all studies. For example, in a study of cervical spine motion, Dehner et al. (2013) did not perform a power analysis to determine the appropriate sample size because due to cost and budgetary constraints the sample consisted of a fixed and maximal number of predetermined participants. Similarly, Mobargha, Ludwig, Ladd, and Hagert (2014) in

their study did not perform a power analysis to determine sample size, because, these scholars used a fixed and predetermined sample size. Data analysis consisted of examining a fixed number of records in the OCR online database at the time of data collection. Additionally, Brezina et al. (2012) showed that a power analysis was not required when the study included all eligible participants in the sample. I did not select a sampling method or conduct a power analysis to determine adequate sample size for this study because I examined and reviewed information relating to all breach cases compiled since the passage of the HITECH law in 2009. In this study, I reviewed all available records in the OCR online database available from years 2009 through the beginning of 2016, rather than sampling only a certain number of records for review. Therefore, conducting a power analysis to determine adequate sample size for this study was not appropriate.

Ethical Research

In both quantitative and qualitative research, ethical issues may arise, and it is the individual researcher's responsibility to behave in an ethical manner (Khan, 2014). An exhaustive list of ethical guidelines do not exist, and ultimately researchers have responsibilities for acting and behaving in an ethical manner (Fujii, 2012). Researchers should refrain from engaging in activities or release any information that may cause undue harm (Khan, 2014). From beginning to end, researchers should behave ethically and responsibly and make ethical choices during each stage of the research process (Wester, 2011). Ethical issues surface at any stage of the process, and some ethical issues may be specific to only certain phases of the process (Blee & Currier, 2011). The ethical

duty of the researcher is to minimize harm to individuals and explain the benefits and potential drawbacks of a study (Wester, 2011).

Although it is the ethical duty of the researcher to reduce participant harm, highlight research benefits and explain potential drawbacks of a study, I did not utilize any individual participants in this research. However, I was mindful of ethical considerations and behave ethically during the entire phase of the study. In addition to ethical behavioral considerations, scholars who engage in research often must obtain approval from internal review committees before a study commence (Blee & Currier, 2011). Similarly, to ensure that I did not violate any institutional ethical guidelines, I submitted my research plans for review and sought approval from Walden University's Institutional Review Committee before commencing the study. Data elements used in this study do not contain sensitive information such as names, organizational records, personal identifying data, or any other private records. All data collected for this study was readily available from a publicly accessible website. However, I will securely maintain all supporting data collected for this study a period of five years. After a period of five years, I will destroy any data or records associated with this study.

Data Collection

Secondary data analysis is the analysis of existing data (Boo & Froelicher, 2013; Irwin, 2013) or information collected for specific reasons or other purposes (Cheng & Phillips, 2014). Analyzing existing data is a cost-effective way to answer new research questions (Boo & Froelicher, 2013; Cheng & Phillips, 2014). Due to digital capabilities and technological advances, the amount electronic information publicly available and

accessible to researchers for scientific research is exponentially growing (Schuster, Anderson, & Brodowsky, 2014). Some scholars recognize the scientific value of secondary research, and there is a growing trend towards the usage of secondary analysis (Irwin, 2013). There are many national governmental databases, electronically available and freely accessible, that contain health related information that researchers can use for a variety of purposes (Boo & Froelicher, 2013).

Instruments

I did not use instruments such as surveys, questionnaires, or other data collection mechanisms for this study but rather utilized an existing publicly available data source. Various publicly available electronic databases exist that contain health-related information (Cheng & Phillips, 2014). DHHS maintains a search and electronic retrieval repository of breach incident information (Hayhurst, 2014). Provisions of the HITECH law mandate that, for all privacy breaches minimally impacting at least 500 people, DHHS must disclose and post a breach directory listing that contains information about the breach of unsecured medical information (Kwon & Johnson, 2013). Additionally, included in the HITECH law are requirements that appropriate officials of covered entities must report details relating to breach incidents to DHHS officials, which result in the exposure of unsecured health records (Lawley, 2012; Liu et al., 2015). In a study of data breaches, Wikina (2014) used information from the DHHS electronic database search and retrieval tool to analyze data breach trends. The goal of Wikina's (2014) study was to identify the main origins, occurrences, and underlying cause of data breaches to potentially help organizational leaders minimize and prevent future breach incidents.

Wikina (2014) found that the majority of the data breach incidents related to theft and data loss rather than technical issues or actions caused by intruders or hackers. In this study, I used information available from OCR to examine and analyze healthcare security incidents and the relationships among various factors related to data privacy breaches.

Scholars conduct two types of research, primary and secondary (Al-Abdallah, 2015). Although some research concepts may apply to both secondary and primary research, in secondary investigative inquiry, researchers analyze and rely upon existing data repositories and available datasets collected by others for different purposes to seek answers and examine research questions (Anderson & Paterson, 2015). With secondary data analysis, scholars conduct new scientific discovery, analyze previously collected information, and derive new interpretations, understandings, findings, and meanings (Fraser, 2015). Additionally, there could be ethical issues that arise when previously collected research data is stagnant and unused (Redman-Maclaren, Mills, & Tommbe, 2014). Therefore, scholars might choose to utilize secondary data to lessen the need for individuals to participate in research studies (Redman-Maclaren et al., 2014).

In addition to other research benefits, when researchers use secondary data there are some potential benefits in terms of cost savings, data collection time, and resources (Anderson & Paterson, 2015; Redman-Maclaren et al., 2014; Whiteside, Mills, & Mccalman, 2012). Researchers can use secondary data as a cost-effective way of identifying and finding answers to research problems saving potentially years of research time required to collect cross-historical or international data (Anderson & Paterson, 2015). Some advocates of secondary data suggest that there are global funding trends

towards reducing research costs and promoting shared open-access to data repositories through research using secondary data (Whiteside et al., 2012). Utilizing secondary data can be less obtrusive than other forms of research (Whiteside et al., 2012) and scholars can use secondary data sources to gain insights about vulnerable or inaccessible populations (Fraser, 2015). Additionally, information and data not readily available might be accessible to researchers via secondary data sources (Brakewood & Poldrack, 2013). Scholars can use secondary data to obtain information and make generalizations about subjects or populations that they may have limited access to (Brakewood & Poldrack, 2013). Thus, for this study, I used secondary data and electronically retrieved from DHHS's website to obtain information and answer a research problem. Upon request, I will provide copies of the raw secondary data utilized and retrieved in this research and followed any specific data management requirements established by Walden University's Institutional Review Board.

DHHS officials aggregate, compile, and publish via the web information relating to unsecured data privacy breaches. DHHS data was appropriate for research data used for this study was publicly available online. Data in the DHHS repository included exposure information relating to unsecured breaches. The dataset contained the following information (a) name of covered entity, (b) state, (c) covered entity type, (d) individuals affected, (e) breach submission date, (f) type of breach, (g) location of breached information, (h) business associate present, and (i) web description.

Data Collection Technique

The data source for this study was information available online from DHHS's publicly accessible breach database. I electronically collected data for the study by downloading the dataset directly from the data privacy breach public website. Disadvantages of performing electronic data collection are that possible technological challenges may arise and in some instances the data repository could timeout, the system might be offline inaccessible, or otherwise unavailable (Mrayyan, 2006). However, despite potential technological challenges with electronic data collection, there could be advantages of utilizing an electronic data collection approach. Over the past decade, the usage and adoption of electronic data collection increased (Lee, 2012).

Budget and resource constraints may contribute to the increasingly growing popularity among scholarly use of electronic data collection (Wright & Ogbuehi, 2014). Some potential benefits of electronic data collection include improved accuracy, timely receipt of information, and data quality improvements by reducing the need for manual secondary data entry (Sauers, McLeod, & Bay, 2012). Therefore, the selected approach for this study was electronic data collection, which I used to examine relationships among factors affecting data privacy breaches. From the data source, I reviewed information relating to data privacy breaches compiled by DHHS personnel since the passage of the HITECH Act. Therefore, I reviewed breaches cases compiled and reported to DHHS during years 2009 through the beginning of year 2016.

Data Analysis Technique

There is no single accepted standard or guideline for determining the best statistical data analysis approach (Tansey, White, Long, & Smith, 1996). The data analysis techniques that I utilized in this study are loglinear statistical testing procedures. I used loglinear statistical procedures to examine the proposed research questions. When examining many categorical variables, there are testing limitations associated with some commonly used statistical procedures such as chi-square analysis and non-parametric procedures (White, Tansey, & Smith, 1994). With categorical variables, test procedures such as chi-square analysis and non-parametric tests are only appropriate in certain situations where researchers are testing relationships between only two variables (White et al., 1994). Chi-square analysis and non-parametric tests are not appropriate for testing multiple simultaneous categorical variables (White et al., 1993). Compared to other techniques such as analysis of variance (ANOVA) and chi square of variance, researchers have access to enhanced statistical capabilities when examining association among multiple categorical variables using loglinear procedures (Olmuş & Erbaş, 2012). Researchers use models to test a set of relationships between a pair of variables while ensuring that other variables are kept constant (White et al., 1994). Loglinear procedures have more statistical power (DeCarlo, Laczniak, Azevedo, & Ramaswami, 2000; Olmuş & Erbaş, 2012). Compared to other statistical techniques, researchers using loglinear procedures can test all potential levels of associations, relationships, and frequencies among variables such as one-way and two-way interactions, and beyond (Olmuş & Erbaş, 2012).

In addition to choosing appropriate statistical test procedures, research considerations might include data handling and cleaning procedures that could affect the outcome of a study. Statistical scholars assert that researchers, as a matter of practice, should detail in research reports any data cleaning and verification processes used (Pomerantseva & Ilicheva, 2011). Lack of data cleaning and screening processes could impact the quality of the data (Ringim, Razalli, & Hasnan, 2012). Data cleaning procedures include checking for unique identifiers, identifying invalid data values, and performing complex reconciliation processes to ensure adherence to certain procedural rules (Pomerantseva & Ilicheva, 2011). Before commencing data analysis, scholars should check the quality and accuracy of information to ensure underlying errors do not exist as data cleaning can positively affect the analytical quality of information (Badara & Saidin, 2014).

Large datasets could be difficult to manage, but researchers could employ electronic software such as Statistical Packages of the Social Sciences (SPSS) to clean and check the data for errors (Badara & Saidin, 2014). In this study, I utilized SPSS software to analyze data, and before analysis, I employed data cleaning procedures such as visually inspecting data, checking data for invalid and missing information, and performing data reconciliation procedures to identify omissions or import errors. Verification of the dataset to ensure information contained in the data does not contain errors or invalid values also occurred. Finally, since the dataset could be relatively large, I used the electronic error checking features of SPSS, to identify, errors, incomplete, missing, and clean the data.

Missing data is problematic (Clarke et al., 2008) and can lead to bias (Cramon et al., 2014; Patrician, Loan, McCarthy, Brosch, & Davey, 2010). Healthcare statutes mandate that DHHS post information regarding certain data breaches of unsecured health information (Kwon & Johnson, 2013). Thus, I assumed the likelihood of missing data in the DHHS dataset is relatively low. However, if the dataset contains any missing data, I employed appropriate methods to manage the missing data elements from the final dataset to reduce any potential problems with the results and minimize the possibility of unwanted bias.

Assuming that information is not randomly missing from the dataset, researchers can use various approaches to account for missing data in their studies (Liu & De, 2015; Roda, Nicolis, Momas, & Guihenneuc, 2014; Young & Johnson, 2013). Methods of handling missing data include techniques such as Bayesian estimation, multiple imputation (MI), complete case analysis (Liu & De, 2015; Roda et al., 2014), and maximum likelihood (ML) estimation, (Liu & De, 2015; Young & Johnson, 2013). Complete case analysis is a common method researchers may deploy to manage missing data (Liu & De, 2015). With complete case analysis, researchers tend to omit missing data or restrict analysis to only available and complete records thereby only utilizing a sub-set of data (Liu & De, 2015; Roda et al., 2014; Young & Johnson, 2013).

Utilizing complete case analysis, researchers can affect the statistical results of their studies leading to biased data or errors (Liu & De, 2015; Roda et al., 2014; Young & Johnson, 2013). Conversely, MI is a conservative approach where researchers do not omit missing data (Roda et al., 2014) but rather retain all usable information available in

the data set (Young & Johnson, 2013). Statistical software packages such as IVEware, Amelia, Stata (Young & Johnson, 2013), SPSS (Liu & De, 2015; Young & Johnson, 2013), Multiple Imputation by Chained Equations (MICE), and statistical analysis system (SAS) (Young & Johnson, 2013) contain MI functionality that scholars can use when their dataset contains missing data (Liu & De, 2015; Young & Johnson, 2013). There are two methods of MI for handling missing data, joint modeling (JM) and fully conditional specification (FCS) (Young & Johnson, 2013).

FCS is appropriate for data containing categorical variables because there is no assumption that normality of all variables exist (Young & Johnson, 2013). The uniqueness of each variable and associated conditional density is an underlying research assumption related to the FCS method, and thus, the FCS technique is more appropriate for categorical variable datasets containing missing information (Young & Johnson, 2013). In studies where the dataset contained categorical variables, scholars used the FCS method of the multiple imputation technique to handle missing data (Demment, Haas, & Olson, 2014; Diepen et al., 2014; Langlois, Lapointe, Valois, & de Leeuw, 2014; Sullivan et al., 2014; Zheng et al., 2015). Similarly, for this study, I managed missing data by deploying the FCS method of the multiple imputation technique.

The accuracy of test results when using some statistical test procedures may depend on certain underlying assumptions that researchers may need to be aware of when performing their work. Two primary assumptions of loglinear techniques are the adequacy of the sample size of the data needed and size of expected frequencies required for the analysis (Öğüş & Yazıcı, 2011). In loglinear analysis, researchers use logarithmic

mathematical functions to analyze distinct elements in contingency tables (Öğüş & Yazıcı, 2011). When performing loglinear testing, the number of samples should consist of minimally five times the number of cases in the dataset and the expected cell frequency size should be sufficient (Öğüş & Yazıcı, 2011). Less than 20% of expected counts in loglinear analysis should have fewer than five observed frequencies, or the researcher will introduce errors affecting the power of the study (Henderson & Stackman, 2010).

For data analysis, I assessed and analyzed the response variables to determine if significant associations among the variables exist. The primary purpose of loglinear analysis is to identify the model that best represents the observed cell frequencies of the variables evaluated (Öğüş & Yazıcı, 2011). All variables are response variables in loglinear analysis; thus, there is no distinction for independent or dependent variables (Pavlović, Milković-Kraus, Jovanović, & Hercigonja-Szekeres, 2012; Sinclair, Emlen, & Freeman, 2012). With loglinear analysis, scientists use contingency tables consisting of categorical variables to analyze the logs of cells, and then starting with the saturated model which consists of all main effects and interactions (Lin & Lin, 2014), select the best-fit or parsimonious model that closely represents the data (Pavlović et al., 2012; Rinke, Wessler, Löb, & Weinmann, 2013).

Scientists can use loglinear models and cross tabulation to evaluate multi-way contingency tables identifying and comparing observed and expected cell frequencies between three or more categorical variables (Onder et al., 2012; Pavlović et al., 2012; Sinclair et al., 2012). Loglinear analysis includes an initial or saturated model containing

of all possible interactions and main effects among all variables (Haveman, Habinek, & Goodman, 2012; Sinclair et al., 2012), effectively eliminating interactions or parameters between variables (Haveman et al., 2012). Using loglinear analysis researchers evaluate and compare multiple hierarchically nested models against a saturated model to determine the most appropriate model that best represents the data (Haveman et al., 2012). Following an elimination or stepwise approach, researchers can use likelihood ratio statistics to assess the estimated frequencies to identify and select the most appropriate model that best fits or represents the data (Pavlović et al., 2012).

Researchers using loglinear techniques can compare main effects and associated interactions of the resulting generated hierarchical models for significance against the saturated model (Sinclair et al., 2012). In a study of parasitic exchange between sedentary and migratory birds, Pérez-Rodríguez, de la Hera, Bensch, and Pérez-Tris (2015) used loglinear analysis techniques to develop a five-way contingency table and examined the relationships between parasitic, seasonal, age, sex and migratory behavior. In their study, Pérez-Rodríguez et al. (2015) generated hierarchical models and found the best-fit model for the data by fitting all corresponding interactions. Additionally, Onder et al. (2012) devised a five-way contingency table to examine the associations and interactions between occupation, area, reason, accident time, and part of body relative to occupational underground coal mine injuries. Onder et al. (2012) used hierarchical loglinear analysis and evaluated the significance of the likelihood ratio to evaluate potential exposure risks of accidents. Çilan (2014) used loglinear and event history analysis with missing data to

analyze variables represented in a five-way contingency table and evaluated the significance levels of resulting models to select the best-fit model.

Similarly, drawing from the work of prior scholars (Çilan, 2014; Onder et al., 2012; Pérez-Rodríguez et al., 2015), using a multi-way contingency table, I summarized secondary breach data retrieved from DHHS and evaluated the association between various data privacy breaches, covered entity types, number of individuals affected, data storage locations, and business associates. Covered entity type is the classification or specific kind of medical organization involved in the data privacy breach. In the table, I summarized cell frequencies representing covered entity type as a health provider, health plan, health clearinghouse, or business associate. Individuals affected by a data breach are the approximate number of people impacted by the security incident. I classified the number of individuals affected by the data breached into a new dummy categorical variable consisting of three categories, breaches affecting up to 50,000 individuals, breaches affecting between 50,001 and 100,000 individuals, or breaches affecting over 100,000 individuals. Location of breached data information is the storage format of the unsecured data consisting of either physical or electronic formats or both manual and electronic formats at the time the breach incident occurred. Business associate present is an indicator of yes or no designating whether or not the security incident involved a third-party vendor or contractor. Many underlying sources may contribute to the cause of data privacy breaches such as theft, accidental loss, hacking, improper exposure of information, or various other causes. Based on the description for type of breach found in the data set, I transformed the type of breach data into a new dummy categorical variable

consisting of three categories, breach involving theft or loss, breach not involving theft or loss, and breach cause unknown or not specified. The resulting cross-tabulation of categorical breakdown of cell frequencies used for data analysis consisted of a 4x4x2x3x3 multi-way contingency table consisting of 288 possible cell combinations. Finally, I used the data represented in the multi-way contingency table to compare the logs of the resulting observed and estimated cell frequencies.

I used SPSS software to examine the response variables and generate various models representing the data. Using an elimination or stepwise approach, I examined the resulting models, identified, and selected the most appropriate model that best fit and represented the data. During data analysis, I used a likelihood statistic to determine the most appropriate model for the data and examined the significance of each resulting model to identify the parsimonious model that most appropriately represented the data. For this study, I did not use any of the variables as an interaction term. Researchers should be cautions when adding an interaction term unless there is a compelling theoretical reason to do so (Dhar & Weinberg, 2015). Problems can arise with the addition of an interaction variable thereby negatively affecting the resulting estimated main and interaction effects leading to unnecessary data analysis or unintended changes that could impact test results (Dhar & Weinberg, 2015).

Errors occur when a researcher violates any underlying assumption but to minimize errors the researcher can collapse and combine variable data elements into new dummy variables (Henderson & Stackman, 2010; Öğüş & Yazıcı, 2011; Tansey et al., 1996), accept the loss of power, or increase sample size (Henderson & Stackman, 2010;

Öğüş & Yazıcı, 2011). Creating cross tabs is also appropriate for verifying that the desired number of expected cell counts align with the assumption (Henderson & Stackman, 2010). Scholars can also delete the number of irrelevant associations, or in rare cases, add a constant to the data when they do not adhere to assumptions but this approach will likely reduce the power of the study (Öğüş & Yazıcı, 2011). To minimize errors or manage assumption violations, I ensured that the size of the dataset was sufficient, created cross tabs, or combined data elements into new dummy variables where appropriate.

In scientific inquiry, scholars may use varying processes to interpret statistical results. Scholars use loglinear statistical procedures to evaluate observed frequencies and expected frequencies within the data (Salter, 2003). For expected and observed frequencies, analysis involves finding the statistical model that best depicts the data (Vaid, 2012). While evaluating the various models in terms of acceptance or rejection of a pair of hypothesis, choosing the best model requires researchers to analyze and compare series of models against a saturated model to determine which model appropriately represents the data (Vaid, 2012). In loglinear testing, researchers compare the homogeneous, conditional, and saturated models (Kamal, Mahmud, Sulong, & Azid, 2014). The most comprehensive model consisting of all main effects and includes both two-way and three-way interactions, is the saturated model (Kamal et al., 2014).

The calculation of the likelihood ratio chi-square (G^2) statistic identifies the presence of a relationship between the expected and observed frequency within a table for a given model generated using loglinear procedures (Vaid, 2012). Using loglinear

statistical procedures, when the resulting statistic (G^2) or p-value is above 0.05 the researcher cannot reject the hypothesis (Vaid, 2012). Both the resulting statistic and significance level is an indication of whether an effect or relationship exist among the variables in the dataset (Salter, 2003). Each line of the resulting output table generated using loglinear procedures depicts different observed and expected frequencies (Salter, 2003). To determine whether to accept or reject the hypothesis, Salter (2003) demonstrated how to use the resulting statistic and the significance value to find a model depicting the relationship that best fit the data. Similarly, in my study to interpret results, I evaluated the resulting model given the G^2 statistic and the significance value and assessed relationship between a given pair of hypotheses.

Reliability and Validity

Reliability and validity relate to the rigorous procedures and processes that researchers use to ensure that they minimize errors or discrepancies in their work (Pfefferbaum et al., 2013). Utilizing reliability and validity procedures, scientists help ensure that their research findings are predictable, repeatable (van Middendorp, Patel, Schuetz, & Joaquim, 2013), scientifically sound, acceptable, and accurate (Pfefferbaum et al., 2013). Reliability and validity affect the trustworthiness or quality of the data (Pfefferbaum et al., 2013). To help achieve reliability in their work, scholars should explain and describe every intrinsic detail of their inquiry or approach (Zohrabi, 2013). Researchers who follow well established and scientifically sound procedures of reliability and validity increase the likelihood that their proposals are accepted (Ellis & Levy, 2009). Reliability is the correctness, consistency (Lakshmi & Mohideen, 2013;

Pfefferbaum et al., 2013), reproducibility (Duxbury, 2012; van Middendorp et al., 2013), dependability, or stability of research results (Duxbury, 2012). In contrast, validity refers to the ability of researchers to formulate meaningful generalizations, inferences, and draw transferable conclusions from the research findings or results (Duxbury, 2012). Thus, it is important that researchers report the outcomes of their findings in terms of reliability and validity (Marais, 2012).

Reliability

Regardless of their role in the process, researchers must consider certain issues to ensure their work is valid (Unluer, 2012). Applying processes of reliability and validity is an important consideration for researchers as their actions help to ensure academic quality, sound conclusions, and meaningful, accurate, and appropriately designed studies (Lakshmi & Mohideen, 2013). Scholars should carefully and methodically select appropriate measurement or assessment tools to ensure reliability and validity in their work and demonstrate scientific rigor and research quality (Christenson et al., 2015). I relied on secondary data for this study and the major threat to reliability relates to the accuracy of the data in the dataset.

DHHS officials are required to submit an annual report to Congress and publically disclose online information relating to privacy breaches of healthcare data caused by covered entities (Classen, Fogarty, & Mier, 2012; Strauss, 2014). Additionally, DHHS officials investigate and resolve written complaints received or submitted via breach reports and other sources (Strauss, 2014). Thus, for this study, due to the annual reporting requirement of Congress and because DHHS investigates and resolves the privacy breach

claims submitted online via the website, I assumed that the online dataset that I utilized for the study contained accurate information. For testing, I did not sample any of the data retrieved via the DHHS website but examined the full dataset that contained information related to breach cases of covered entities reported since the passage of the HITECH law through the beginning of 2016. Since I did not employ any sampling techniques, for this study, I assumed there are no threats to reliability related to sampling.

Validity

In addition to reliability considerations, issues related to validity might affect the outcome of research results or quality of a study. Research results may have either internal or external validity (Lakshmi & Mohideen, 2013). Internal validity is the researcher's ability to form inferences (Sikorskii & Noble, 2013) or to legitimately, effectively, and accurately measure what they intend to measure (Price & Murnan, 2004). Internal validity relates to the congruency of research outcomes and findings of a study (Zohrabi, 2013). Conversely, external validity relates to the researcher's ability to generalize or apply findings and results to larger populations, groups, or other settings (Lakshmi & Mohideen, 2013; Sikorskii & Noble, 2013). With external validity, researchers have a certain level of confidence that findings can extend to different populations, settings, situations, and groups (Zohrabi, 2013).

Although scholars may use various definitions to describe validity within research, essentially, validity relates to the overall accuracy and creditability of a study (Pfefferbaum et al., 2013). In this study, I managed threats to internal validity by relying on a governmental database for data collection that was appropriate for evaluating and

examining privacy breaches. Due to varying U.S. state reporting and disclosure laws, there is no single repository that includes comprehensive information about all data breaches (Adebayo, 2012). Wikina (2014) used DHHS's publicly available dataset to identify the origin and likely cause of healthcare privacy breaches. The DHHS online public dataset was also relevant for this study. I used the dataset to examine information relating to healthcare breaches to identify possible relationships that may exist among factors that might contribute to the cause of data privacy breaches. The DHHS dataset contains information about data privacy breaches relating to covered entities within the U.S. healthcare industry. However, breaches of private or sensitive information could occur in other industries such a financial, telecommunications, utilities, and beyond. Thus, in terms of external validity, findings and generalizations made in regards to this study are limited to U.S. healthcare entities and may not extend to other industries or healthcare sectors in other countries.

Transition and Summary

In Section 2, I discussed the purpose of the study and presented the rationale for choosing a quantitative loglinear research approach over other research methods and design approaches. I explained the underlying assumptions applicable to loglinear techniques and noted why loglinear statistical analytical procedures were suitable for this research. Section 2 also contained a description of the population selected for the study, and I provided an overview of the type of information contained in the DHHS secondary data source that I utilized for this research. I also explained the rationale for choosing to use secondary information contained in the DHHS online governmental database to

conduct the study. I presented ethical considerations and noted potential conflicts of interest that could be relevant to this research. Outlined in Section 2 were specific data collection and analysis procedures I followed in this study. In Section 3, I present the findings of the study and discuss the how the findings from this research might apply to information security practices in the U.S. healthcare sector.

Section 3: Application to Professional Practice and Implications for Change

Section 3 includes an overview of the results and findings relating to the study. Outlined in Section 3 is a detailed discussion of the hierarchical and general loglinear analysis research procedures. Provided in Section 3 is an explanation of the research findings and a discussion of how the study findings confirm or contradict prior research on data privacy breaches. Section 3 concludes with a discussion of recommendation for future research and application to social change and business practice.

Overview of Study

The purpose of this quantitative loglinear study was to examine the association between data privacy breaches, business associates, covered entities, the number of individual affected, and data storage locations. The variables were data privacy breaches, covered entity types, number of individuals affected, storage location of breach data, and business associates. Research findings revealed the acceptance of the alternative hypothesis. Therefore, I rejected the null hypothesis. Using the hierarchical loglinear model backward elimination procedure within SPSS, I identified the most appropriate unsaturated model that best represented the data. The resulting hierarchical loglinear procedure showed four models fit the data. Among the four models fitting the data, the results of the general loglinear procedure indicated that the model containing all main effects and a model consisting of the four-way interaction denoted as *business associate present * no. of individuals affected * data storage location * type of breach* best fit the dataset. The analysis of the research results using the general loglinear procedure for the resulting unsaturated model revealed that all main effects consisting of variables covered

entity type, number of individuals affected, data storage location, type of data breach, and business associate present were significant.

Presentation of the Findings

The focus of this research was to examine the overall association between five categorical variables that included data privacy breaches, covered entity types, number of individuals affected, storage location of breach data, and business associates. In order to perform the analysis, I downloaded information about data breaches affecting more than 500 individuals from OCR's website in the form of a text file and imported the text file into SPSS. Next, using the transform feature within SPSS, I recoded the variables retrieved from the imported dataset into five categorical variables.

Test of Assumptions

Assumptions for loglinear procedures are that the number of samples consist of at least five times the number of cases in the dataset, the expected cell frequency size should be sufficient (Öğüş & Yazıcı, 2011), and no more than 20% of expected counts should have fewer than five observed frequencies (Henderson & Stackman, 2010; Henderson, Stackman, & Koh, 2013). However, a review of the resulting SPSS output for 4x4x2x3x3 multiway contingency table showed that there were many expected frequencies that contained cell values of less than one and more than 20% of expected counts had fewer than five observed frequencies. For loglinear analysis, researchers can delete the number of irrelevant associations or add a constant to the dataset when assumption violations occur (Öğüş & Yazıcı, 2011). Possible remedies for assumption violations when using loglinear analysis also include collapsing or combining variable data elements into new

dummy variables (Henderson & Stackman, 2010; Henderson et al., 2013; Öğüş & Yazıcı, 2011; Tansey et al., 1996), accept the loss of power, or increase sample size (Henderson & Stackman, 2010; Öğüş & Yazıcı, 2011). Thus, to remedy the assumption violations, I added a constant of one to the dataset and collapsed the number of levels for the covered entity, breach storage location, number of individuals affected, and type of data privacy breach into new dummy variables. Combining the levels among the variables resulted in a new 2x2x2x2x2 contingency table consisting of 32 possible cell combinations. The type of data privacy breach variable included two levels denoted as breach cause associated with theft or loss or breach cause not associated with theft or loss. The individuals affected variable consisted of two levels that included breach affecting up to 5,000 individuals and breach affecting more than 5,000 individuals. The covered entity type variable consisted of two levels, denoted as a healthcare provider or non-healthcare provider, such as a health plan, business associate, or clearinghouse. I also combined the data storage location variable into two levels consisting of electronic data storage format only and a combination of electronic, physical, or other storage formats. The business associates variable was not changed and consisted of a *yes* or *no* indicator designating whether or not the security incident involved a third-party vendor or contractor. Table 1 includes a description of the variables used for the study. As shown in Table 1, all variables used in the study contained categories consisting of two levels.

Table 1

Description of Variables Used in the Study

Variable	Variable descriptors
Business associate present	Yes
	No
Covered entity type	Healthcare provider
	None healthcare provider or other covered entity
Data storage location	Electronic data storage location only
	Combination of physical, electronic, or other data storage location only
No. of individuals affected	Breach affected 5000 or less individuals
	Breach affected more than 5000 individuals
Type of data privacy breach	Breach cause associated with theft or loss
	Breach cause not associated with theft or loss

Next, I used the data represented in the multi-way contingency table to compare the logs of the resulting observed and estimated cell frequencies to determine if associations among the data existed. Table 2 depicts the resulting contingency table and includes expected and observed cell frequencies for each of the variables. The observed and expected cell frequencies of the revised contingency table met all assumptions associated with loglinear analysis procedures.

Table 2

Cell Counts and Residuals

Covered entity	Individuals affected	Data storage location	Type of data privacy breach	BP	Observed		Expected		RS	Std. RS
					Count[a]	%	Count	%		
Health-care provider	Breach affected 5000 or less individuals	Electronic data storage location only	Breach cause associated with theft or loss	Yes	3.0	.0%	3.0	.0%	0.0	0.0
				No	1390.0	15.5%	1390.0	15.5%	0.0	0.0
			Breach cause not associated with theft or loss	Yes	7.0	.1%	7.0	.1%	0.0	0.0
				No	915.0	10.2%	915.0	10.2%	0.0	0.0
		Combination of physical, electronic, or other data storage location only	Breach cause associated with theft or loss	Yes	8.0	.1%	8.0	.1%	0.0	0.0
				No	1347.0	15.1%	1347.0	15.1%	0.0	0.0
			Breach cause not associated with theft or loss	Yes	1.0	.0%	1.0	.0%	0.0	0.0
				No	713.0	8.0%	713.0	8.0%	0.0	0.0
	Breach Affected more than 5000 individuals	electronic data storage location only	Breach cause associated with theft or loss	Yes	1.0	.0%	1.0	.0%	0.0	0.0
				No	736.0	8.2%	736.0	8.2%	0.0	0.0
			Breach cause not associated with theft or loss	Yes	7.0	.1%	7.0	.1%	0.0	0.0
				No	359.0	4.0%	359.0	4.0%	0.0	0.0
		Combination of physical, electronic, or other data storage location only	Breach cause associated with theft or loss	Yes	1.0	.0%	1.0	.0%	0.0	0.0
				No	365.0	4.1%	365.0	4.1%	0.0	0.0
			Breach cause not associated with theft or loss	Yes	1.0	.0%	1.0	.0%	0.0	0.0
				No	206.0	2.3%	206.0	2.3%	0.0	0.0

(table continues)

Covered entity	Individuals affected	Data storage location	Type of data privacy breach	BP	Observed		Expected		RS	Std. RS
					Count[a]	%	Count[a]	%		
None health-care provider other covered entity	Breach affected 5000 or less individuals	Electronic data storage location only	Breach cause associated with theft or loss	Yes	238.0	2.7%	238.0	2.7%	0.0	0.0
				No	64.0	.7%	64.0	.7%	0.0	0.0
			Breach cause not associated with theft or loss	Yes	225.0	2.5%	225.0	2.5%	0.0	0.0
				No	155.0	1.7%	155.0	1.7%	0.0	0.0
		Combination of physical, electronic, or other data storage location only	Breach cause associated with theft or loss	Yes	323.0	3.6%	323.0	3.6%	0.0	0.0
				No	142.0	1.6%	142.0	1.6%	0.0	0.0
			Breach cause not associated with theft or loss	Yes	284.0	3.2%	284.0	3.2%	0.0	0.0
				No	289.0	3.2%	289.0	3.2%	0.0	0.0
	Breach affected more than 5000 individuals	Electronic data storage location only	Breach cause associated with theft or loss	Yes	197.0	2.2%	197.0	2.2%	0.0	0.0
				No	88.0	1.0%	88.0	1.0%	0.0	0.0
			Breach cause not associated with theft or loss	Yes	143.0	1.6%	143.0	1.6%	0.0	0.0
				No	178.0	2.0%	178.0	2.0%	0.0	0.0
		Combination of physical, electronic, or other data storage location only	Breach cause associated with theft or loss	Yes	235.0	2.6%	235.0	2.6%	0.0	0.0
				No	64.0	.7%	64.0	.7%	0.0	0.0
			Breach cause not associated with theft or loss	Yes	138.0	1.5%	138.0	1.5%	0.0	0.0
				No	148.0	1.7%	148.0	1.7%	0.0	0.0

Note. a. For saturated models, 1.000 has been added to all observed cells. BP=Business Associate Present, RS=Residuals, Std RS=Standard Residuals

Descriptive Statistics

The type of data privacy breach variable included three levels denoted as (a) breach cause associated with theft or loss, (b) breach cause not associated with theft or

loss, (c) and breach associated with an unknown or unspecified cause. Individuals affected represented the approximate number of people impacted by the security incident. The individuals affected variable consisted of three levels including (a) up to 50,000 individuals affected, (b) between 50,001 and 100,000 individuals affected, and (c) the breach having affected over 100,000 individuals. Business associates variable consisted of a *yes* or *no* indicator designating whether or not the security incident involved a third-party vendor or contractor. The covered entity type variable was an indicator of the classification or specific kind of medical organization involved in the data privacy breach that consisted of (a) health provider, (b) health plan, (c) health clearinghouse, (d) or business associate. Location of data breached information variable represented the format of the unsecured data at the time of the breach incident that consisted of physical only, electronic format only, a combination of both electronic and physical formats, or an unknown or otherwise not specified breach format. Table 3 shows the descriptive statistics for the coded imported dataset. Descriptive statistics showed that the *N* value, representative of the number of samples in the data, for all of the variables were different with values ranging from 1462 to 1498. As depicted in Table 3, different values of *N* indicate that the dataset contained missing elements.

Table 3

Descriptive Statistics for OCR Data Imported Dataset

Variable	*N*	Minimum	Maximum	Mean	Std. deviation
Covered entity type	1462	1	4	1.7	1.16332
No. of individuals affected	1475	1	3	1.102	0.40914
Business associate present	1498	1	2	1.798	0.40183
Data storage location	1485	1	4	1.951	1.20852
Type of data privacy breach	1482	1	3	1.833	0.98143
Valid *N* (listwise)	1449				

From the descriptive statistics, I determined that four of the variables included in the imported OCR dataset contained missing records and data elements. Thus, to address the missing information, I used the multiple imputation features within SPSS to analyze the missing patterns of data. The FCS multiple imputation approach is appropriate for categorical variables containing missing information because there is no assumption of normality among the variables (Young & Johnson, 2013). For the missing data analysis, I configured SPSS to identify variables that contained at least .0001% of missing information. Table 4 depicts missing records contained in the dataset file. The covered entity type variable contained 2.4% of missing data, and the other variables had at least 1% of missing information.

Table 4

Missing Variable Summary [a,b]

Variable	Missing		Valid *N*
	N	Percent	
Covered entity type	36	2.40%	1462
No. of individuals affected	23	1.50%	1475
Type of data privacy breach	16	1.10%	1482
Data storage location	13	0.90%	1485

Note. a. Maximum number of variables shown: 25 b. Minimum percentage of missing values for variable to be included: .0%

After identifying the missing patterns of records within the original data file, I ran the FCS multiple imputation procedure within SPSS and imputed five missing datasets. Table 5 shows the number of imputed values generated for each of the variables containing missing data included in the original data file. During the study, I utilized the resulting imputed dataset, which I generated using the SPSS FCS multiple imputation

procedure for all remaining analysis. SPSS imputed 180 values for covered entity type, 115 values for number of individuals affected, 65 values for data storage location and 80 values for type of data privacy breach variable.

Table 5

Resulting Imputation for Missing Values

Variable	Missing values	Imputed values
Covered entity type	36	180
No. of individuals affected	23	115
Data storage location	13	65
Type of data privacy breach	16	80

The purpose of the study was to determine if associations existed among the five categorical variables. I used general loglinear analysis procedures within SPSS to assess the associations, interactions, and significance among the variables. Loglinear analysis is an analytical procedure researchers use to assess significance, interactions (Haque et al., 2012), relationships, and associations among categorical variables and cell frequencies (Haque et al., 2012; Okoli, Onyeagu, & Osuji, 2015). With loglinear analysis procedures, all variables are response variables; there is no distinction between exploratory or response variables (Okoli et al., 2015). The initial hierarchical loglinear analysis procedure consisted of five categorical variables resulting in a 4x4x2x3x3 multiway contingency table with 288 possible cell combinations.

Inferential Results

Using loglinear analysis scholars examine associations and interactions among categorical variables (Henderson et al., 2013; Onder et al., 2012). Utilizing loglinear techniques, scholars can analyze different hierarchical models against a saturated model to determine the most appropriate model that best represents the data (Haveman et al., 2012). The saturated model is the most comprehensive and complete model which includes all potential combinations of associations and interactions among the various variables (Okoli et al., 2015). Saturated models fit the data perfectly and include all main effects and interactions (Onder et al., 2012).

The research question related to this study was, what is the association between data privacy breaches, data storage locations, business associates, covered entities, and number of individuals affected? To answer the research question, I constructed a five-way contingency table and used loglinear analysis to determine the most appropriate hierarchical unsaturated model that best represented the associations among the five variables. When conducting analysis if the resulting *p*-value is less than the chosen significance level, researchers will reject the null hypothesis and indicate that a significant relationship exist (Olmuş & Erbaş, 2012). To test the association, I selected a significance value of .05. In terms of the research question, the hierarchical loglinear analysis procedure for K-way and first through fourth higher order effects included in the model yielded a significance value of .0.000, $p > .05$ for the both the likelihood ratio and Pearson chi-square statistics see Table 6. For the saturated model, a significance value of 0.000 indicates a relationship or association exist among the five variables. Thus, based

upon the significance value of .000, I rejected the null hypothesis that there is not an association between data privacy breaches, data storage locations, business associates, covered entities, and number of individuals affected by a data breach. Conversely, I accepted the alternative hypothesis that there is an association between data privacy breaches, data storage locations, business associates, covered entities, and number of individuals affected by a data breach. However, for $K = 5$, $df = 1$, the first order effects the results were not significant at $p = .853$, $p > .05$ see Table 6. For the purposes of loglinear analysis, the saturated model, which includes all main effects and interactions is not the ideal model due to its complexity in terms of interpreting research results (Haque et al., 2012).

Table 6

Hierarchical Loglinear Analysis K-Way and Higher-Order Effects

K		*df*	Likelihood ratio		Pearson		Number of iterations
			Chi-Square	Sig.	Chi-Square	Sig.	
K-way and higher order effects[a]	1	31	11715.624	0.000	14485.977	0.000	0
	2	26	5707.204	0.000	5422.841	0.000	2
	3	16	77.720	.000	104.431	.000	11
	4	6	32.112	.000	32.343	.000	7
	5	1	.034	.853	.034	.853	5
K-way Effects[b]	1	5	6008.419	0.000	9063.137	0.000	0
	2	10	5629.484	0.000	5318.410	0.000	0
	3	10	45.608	.000	72.088	.000	0
	4	5	32.078	.000	32.309	.000	0
	5	1	.034	.853	.034	.853	0

Note. df used for these tests have NOT been adjusted for structural or sampling zeros. Tests using these *df* may be conservative. a. Tests that k-way and higher order effects are zero. b. Tests that k-way effects are zero.

Saturated models are complex and difficult to examine, and therefore, researchers prefer unsaturated models when interpreting results because unsaturated models are

straight-forward and easier to interpret (Haque et al., 2012). Alternatively, to interpret results researchers in a backward elimination or stepwise approach, remove and test variables from the saturated model to assess whether the removal of variables significantly affect the model (Haque et al., 2012; Kamal et al., 2014; Olmuş & Erbaş, 2012; Pavlović et al., 2012). Researchers examine the resulting likelihood ratio statistic to identify the most appropriate unsaturated model that best fits or represents the data (Olmuş & Erbaş, 2012; Pavlović et al., 2012). Both the Pearson chi-square and likelihood ratio statistics are indicators that measure the goodness of fit tests resulting from a model (Haque et al., 2012). Therefore, in order to ensure accurate and better interpretation of the results and I used the SPSS hierarchical loglinear model selection procedure and identified a more appropriate model that fit the data.

Using the hierarchical loglinear model backward elimination feature within SPSS, I configured SPSS to identify the most appropriate unsaturated model that best represented the data. The resulting hierarchical loglinear procedure showed four possible models fit the data. The hierarchical loglinear procedure revealed that models which included a three way association and three four-way associations all fit the dataset. The analysis revealed that three four way association models consisting of *(a) covered entity type*number of individuals affected*type of data privacy breach*business associates, (b) covered entity type*data storage location*type of data privacy breach*business associates, (c) and type of data privacy breach*business associates*number of individuals affected*data storage location* possibly fit the observed dataset. Additionally, the backward elimination procedure revealed that a three way association model

consisting of variables *covered entity type*number of individuals affected*data storage location* also potentially fit the observed dataset. Shown in Table 7 are the results of the goodness of fit tests for the hierarchical loglinear model selection backward elimination procedure. As shown in Table 7, the resulting *p*-value or significance value was .998 with a least likelihood ratio and Pearson chi-square statistic of estimate of .042. The resulting *p*-value of .998 was non-significant which is representative of a good model fit. A non-significant *p*-value indicates that the model is a good fit for the data (Grzybek et al., 2015; Henderson & Stackman, 2010). Therefore, all four models resulting from the SPSS backward elimination procedure could likely fit the dataset.

Table 7

Goodness-of-Fit Tests

	Chi-Square	*df*	Sig.
Likelihood ratio	.042	3	.998
Pearson	.042	3	.998

Note. Sig. = *p*-value

When performing loglinear analysis, researchers use contingency tables (Lin & Lin, 2014) or cross-tabulation tables which denote the frequency of variable distributions (Okoli et al., 2015). In loglinear analysis, scholars generate contingency tables consisting of categorical variables to analyze the logs of cells (Lin & Lin, 2014) and utilize loglinear procedures to determine the magnitude and statistical significance of variables (Haque et al., 2012). Next, starting with the saturated model that includes all main effects and interactions (Lin & Lin, 2014) researchers select the best-fit or parsimonious model that closely represents the data (Pavlović et al., 2012; Rinke et al., 2013). Since the results of

the SPSS backward elimination indicated that four possible unsaturated models all fit the observed dataset, I performed additional procedures to identify and select which model among the four identified models best represented the dataset. From the four models, I then selected the overall chosen model representative of the most parsimonious best fitting dataset.

To determine which of the four models generated using the loglinear model selection procedure was the most parsimonious model, I ran the general loglinear procedure. Using the general loglinear procedure, I tested all four unsaturated models resulting from the loglinear hierarchical model selection procedure. I also tested the model fit using a single custom model consisting of all four interactions included in each of the four models. For each of the models, I compared the likelihood ratio statistic, Pearson chi-square statistic, and significance value or *p*-value. Table 8 contains the goodness of fit tests results for each of the models. To assess the fit of a model, researchers examine resulting observed and expected frequencies generated by loglinear models (Kamal et al., 2014). Additionally, scholars can examine the value of the likelihood ratio statistic (Haque et al., 2012; Kamal et al., 2014; Petitjean, Allison, & Webb, 2014) and *p*-value statistic to assess whether the model fit the data (Haque et al., 2012; Kamal et al., 2014). As shown in Table 8, except for the model consisting of all combined model interactions, an examination of the goodness of fit revealed that the *p*-value for all models were significant $p < .005$. Next, to assess model fitness, I examined the resulting observed and expected cell frequencies for each of the models. With the exception of the Model 3 represented by *Bus_Inv_REC * No_Indv_Breach_RECD **

*Breach_LOC_RCDD * Breach_RCTFL,* an examination of resulting cell frequencies in each of the contingency tables showed that four of the tested models resulted in expected cell frequencies values of zero. To meet the assumption requirements for loglinear analysis, the chosen model should contain no more than 20% of expected cell frequency values that have fewer than five cells (Henderson et al., 2013). Therefore, I determined that the best fit model containing all main effects and a four-way interaction for the dataset was Model 3 denoted as *Bus_Inv_REC * No_Indv_Breach_RECD * Breach_LOC_RCDD * Breach_RCTFL* yielding a likelihood ratio statistic of 5458.89 and Pearson chi-square statistic of 4916.94 with 14 *df* (*p*-values of 0.000). I utilized Model 3 which best fit the data for the remainder of the analysis.

When there are no assumption violations of the data, the chi-square statistic is the recommended statistic researchers should use to assess the model fit (Zhu, Walter, Rosenbaum, Russell, & Raina, 2006). Additionally, researchers can also examine the values of standardized residuals resulting from loglinear models to determine whether a model is a good fit and smaller residuals likely indicate a good fit (Kamal et al., 2014). For Model 3, all resulting expected cell counts generated were greater than one, and there were no resulting expected cell counts of less than five. Additionally, Model 3 showed that the adjusted residuals were approximately normally distributed see Figure 1. Model 3 also had the highest Pearson chi-square statistic of 4916.94 indicative of a good fit to the data. An observation and analysis of the standardized residuals resulting from the loglinear models showed that the chosen model denoted as *Bus_Inv_REC **

*No_Indv_Breach_RECD * Breach_LOC_RCDD * Breach_RCTFL* had smaller standardized residual values.

Table 8

Goodness-of-Fit Tests for Unsaturated General Loglinear Models

Model no.	Model description	Likelihood ratio	Pearson chi-square	*df*	Pearson chi-square *p*-value	Likelihood ratio *p*-value
1.	Cov_Entity_RECD * No_Indv_Breach_RECD * Breach_LOC_RCDD	5313.303	4902.573	22	0.000	0.000
2.	Cov_Entity_RECD * Bus_Inv_REC * Breach_LOC_RCDD * Breach_RCTFL	336.791	337.641	15	.000	.000
3.	Bus_Inv_REC * No_Indv_Breach_RECD * Breach_LOC_RCDD * Breach_RCTFL	5458.897	4916.948	15	0.000	0.000
4.	Cov_Entity_RECD * Bus_Inv_REC * No_Indv_Breach_RECD * Breach_RCTFL	295.305	286.615	15	.000	.000
5.	Cov_Entity_RECD * Bus_Inv_REC * Breach_LOC_RCDD * Breach_RCTFL + Cov_Entity_RECD * No_Indv_Breach_RECD * Breach_LOC_RCDD + Bus_Inv_REC * No_Indv_Breach_RECD * Breach_LOC_RCDD * Breach_RCTFL + Cov_Entity_RECD * Bus_Inv_REC * No_Indv_Breach_RECD * Breach_RCTFL	.025	.025	3	.999	.999

Note. Cov_Entity_RECD: Covered entity type, No_Indv_Breach_RECD: No. of individuals affected, Breach_LOC_RCDD: Data storage location, Breach_RCTF: Breach Type, Bus_Inv_REC: Business associate present; *df* = degrees of freedom, Model no.= Model number.

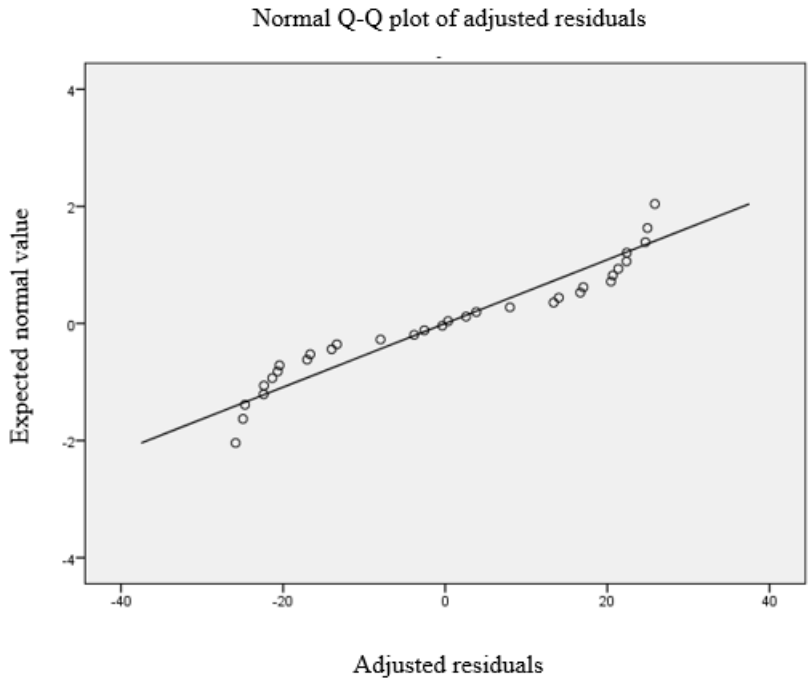

Figure 1. Adjusted Residuals Normally Distributed

Using SPSS Statistics hierarchical loglinear model selection procedure with a backwards elimination stepwise procedure, I performed a five-way loglinear analysis procedure and determined that an unsaturated model consisting of *Bus_Inv_REC * No_Indv_Breach_RECD * Breach_LOC_RCDD * Breach_RCTFL* best fit the dataset. The model had a likelihood ratio of likelihood ratio statistic of 5458.89 and Pearson chi-square statistic of 4916.94 with 14 *df* (*p*-values of 0.000). Presented in Table 9 are partial associations resulting from the model hierarchical selection procedure. Using a significance *P*-value of $p < .05$, the hierarchical selection procedure revealed that there were 18 significant partial associations. The analysis showed one significant four-way association among *covered entity type, data storage location, type of data breach, and*

business associate present, $p = .001$. Significant three-way higher order associations included (a) *covered entity type, no. of individuals affected, and data storage location*, $p = .005$; (b) *no. of individuals affected, data storage location, and type of data breach*, $p = .026$; (c) *no. of individuals affected, data storage location, and business associate present*, $p = .000$; and (d) *covered entity type, type of data breach, and business associate present*, $p = .000$. Among the two-way effects, significant associations included (a) *covered entity type and no. of individuals affected, p = .000; (b) covered entity type and data storage location*, $p = .000$; (c) *no. of individuals affected and data storage location*, $p = .000$; (d) *covered entity type and type of data breach*, $p = .000$; (e) *no. of individuals affected and type of data breach*, $p = .000$; (f) *data storage location and type of data breach*, $p = .003$; (g) *covered entity type and business associate present*, $p = .000$; and (h) *type of data breach and business associate present*, $p = .000$. Additionally, in the chosen unsaturated model, all main effects *covered entity type, no. of individuals affected, data storage location, type of data breach*, and *business associate present* were significant at $p = .000$.

Table 9

Partial Associations for Loglinear Hierarchical Selection Procedure

Effect	*df*	Partial Chi-Square	Sig.	Number of iterations
Cov_Entity_RECD*No_Indv_Breach_RECD*Breach_LOC_RCDD*Breach_RCTF	1	0.000	1.000	3
Cov_Entity_RECD*No_Indv_Breach_RECD*Breach_LOC_RCDD*Bus_Inv_REC	1	.009	.923	8
Cov_Entity_RECD*No_Indv_Breach_RECD*Breach_RCTFL*Bus_Inv_REC	1	3.113	.078	6
Cov_Entity_RECD*Breach_LOC_RCDD*Breach_RCTFL*Bus_Inv_REC	1	10.197	.001*	5
No_Indv_Breach_RECD*Breach_LOC_RCDD*Breach_RCTFL*Bus_Inv_REC	1	1.840	.175	3
Cov_Entity_RECD*No_Indv_Breach_RECD*Breach_LOC_RCDD	1	8.025	.005*	5

(table continues)

Effect	*df*	Partial Chi-Square	Sig.	Number of iterations
Cov_Entity_RECD*No_Indv_Breach_RECD*Breach_RCTFL	1	.211	.646	7
Cov_Entity_RECD*Breach_LOC_RCDD*Breach_RCTFL	1	.578	.447	7
No_Indv_Breach_RECD*Breach_LOC_RCDD*Breach_RCTFL	1	4.951	.026*	6
Cov_Entity_RECD*No_Indv_Breach_RECD*Bus_Inv_REC	1	.450	.502	7
Cov_Entity_RECD*Breach_LOC_RCDD*Bus_Inv_REC	1	.160	.690	8
No_Indv_Breach_RECD*Breach_LOC_RCDD*Bus_Inv_REC	1	20.821	.000*	5
Cov_Entity_RECD*Breach_RCTFL*Bus_Inv_REC	1	14.880	.000*	10
No_Indv_Breach_RECD*Breach_RCTFL*Bus_Inv_REC	1	2.577	.108	7
Breach_LOC_RCDD*Breach_RCTFL*Bus_Inv_REC	1	1.043	.307	7
Cov_Entity_RECD*No_Indv_Breach_RECD	1	127.319	.000*	10
Cov_Entity_RECD*Breach_LOC_RCDD	1	100.721	.000*	10
No_Indv_Breach_RECD*Breach_LOC_RCDD	1	123.296	.000*	11
Cov_Entity_RECD*Breach_RCTFL	1	399.578	.000*	8
No_Indv_Breach_RECD*Breach_RCTFL	1	14.449	.000*	10
Breach_LOC_RCDD*Breach_RCTFL	1	8.595	.003*	10
Cov_Entity_RECD*Bus_Inv_REC	1	4853.452	.000*	5
No_Indv_Breach_RECD*Bus_Inv_REC	1	3.699	.054	10
Breach_LOC_RCDD*Bus_Inv_REC	1	3.166	.075	10
Breach_RCTFL*Bus_Inv_REC	1	153.352	.000*	9
Cov_Entity_RECD	1	1133.484	.000*	2
No_Indv_Breach_RECD	1	1199.251	.000*	2
Breach_LOC_RCDD	1	21.765	.000*	2
Breach_RCTFL	1	230.717	.000*	2
Bus_Inv_REC	1	3423.202	.000*	2

Note: Cov_Entity_RECD: Covered entity type, No_Indv_Breach_RECD: No. of individuals affected, Breach_LOC_RCDD:Data storage location, Breach_RCTF: Breach Type, Bus_Inv_REC: Business associate present. *Significant at the $p < 0.05$ level. Sig = p value

To determine which of the variables are most important in a parsimonious model researchers use parameter estimates (Kamal et al., 2014). Parameter estimates, also known as effect sizes, are representative of odd ratios that measure the strength of variable associations (Zhu et al., 2006). Given a comparison group, odds are the probability or overall chance that a given event will occur versus the probability that the

event will not occur (Onder et al., 2012). Odds ratios indicate the relative likelihood that a given event will occur in comparison with other events (Haque et al., 2012; Olmuş & Erbaş, 2012). An odds ratio is a type or common measure of effect size (Lin & Lin, 2014; Olmuş & Erbaş, 2012; Onder et al., 2012) which relate to parameter estimates (Kamal et al., 2014). Odds ratio values larger than one indicate a positive relationship (Zhu et al., 2006) or positive association (Kamal et al., 2014) among the variables which increase the odds (Onder et al., 2012). Conversely, odds ratio values under one represent a negative association (Kamal et al., 2014; Zhu et al., 2006) or decreases the odds (Onder et al., 2012). An odds ratio value of one mean that there is not an effect or association among the variables (Kamal et al., 2014; Onder et al., 2012) or indicates that there is an equal chance that an event will occur in either scenario (Olmuş & Erbaş, 2012). More significant positive parameter estimates closely predict cell cases and significant negative, parameter estimates possibly may predict fewer cases (Kamal et al., 2014). The resulting unsaturated model best fitting the data showed significant parameter estimates or odds ratio values. Researchers can also use Z statistics, which test the effect size, to determine the relative strength of an association (Kamal et al., 2014). Shown in Table 10 are the parameter estimates resulting from the general loglinear model for all main effects of the chosen parsimonious model.

Table 10

Results of the General Loglinear Model for all Main Effects

Parameter estimates	Estimate	Std. error	*Z*	Sig.
Constant	4.736			
[Covered entity type = healthcare provider]	.736	.023	32.566	.000*
[Business associate involvement = yes]	-.944	.101	-9.371	.000*

(table continues)

Parameter estimates	Estimate	Std. error	*Z*	Sig.
[No. of individuals affected = breach affected 5000 or less individuals]	1.044	.062	16.847	.000*
[Data storage location = electronic data storage location only]	.419	.069	6.100	.000*
[Type of data privacy breach = breach cause associated with theft or loss]	.193	.072	2.683	.007*

Note: *Significant at the $p < 0.05$ level, Sig. = *p*-value

Using a significance value or *P*-value of $p < .05$, the analysis resulting from the general loglinear procedure showed significant parameter estimates or odds values for all main effects in the parsimonious model. As shown in Table 10, of the main effects no. of individuals affected had the highest estimate or odds at 1.044, $p = .000$. An estimate or odds value of 1.044 indicates that in data breach incidents, it is 1.044 more times likely than not, that a data privacy breach will affect up to 5000 individuals. Study findings somewhat support the assertion of Ozair et al. (2015) that data breaches resulting from unwanted exposure of patient information may affect the privacy and confidentiality of individuals. Results that data breaches 1.044 times more likely that not affect individuals also appear to affirm Perakslis (2014) claim that data breaches, in terms of patient safety, may affect individuals, likely up to 5000 individuals, because data privacy breaches can affect some medical devices used in patient treatment that remotely monitor and diagnosis certain medical conditions. The loglinear analysis also showed an estimate of -.944, $p = .000$ for business associate involvement indicating that in roughly 94% of the time business associates are not involved data privacy breaches. Research results are inconsistent with prior research findings of Willey and White (2013) noted that in 2011, external agents or otherwise third party business associates represented 98% of breach

incidents. Test results also appear in contradiction with the research results of Liu et al. (2015) who found that based upon the types and characteristics of breach incidents business associates or external third-party vendors represented 28 % of all reported breach cases examined.

The estimate value for covered entity type was .736, $p = .000$ which showed that about 74% of data breach incidents involve healthcare providers. Findings indicating approximately 74% of data breaches involve healthcare providers, rather than involve non-healthcare providers, such as a health plan or clearinghouse, appear to confirm the assertion of Perakslis (2014), In a prior study, Perakslis (2014) highlighted that malicious activity taken against medical institutions, clinical practices, and hospitals represented approximately 72% of attacks and other attacks targeting pharmaceutical companies, health plans the other medical facilities represented 28% of attacks.

For the data storage location variable, the estimate value was.419, $p = .000$, which signaled that only about 42% of data privacy breaches result in exposure of data stored only in electronic format. Study findings were somewhat consistent with the findings of Wikina (2014) who found that the source of breached records for covered entities and business associates were physical documents but also included portable electronic devices such as laptops, and removal media. Findings also seem to confirm assertions of Chang and Wang (2011) who noted that organizational leaders increasingly rely on information systems to operate their businesses, but, individuals can expose information that resides within these systems resulting in unwanted exposures, losses, and data breaches. Research findings that about 42% of data privacy breaches result in exposure of

data stored in some type of electronic format is also consistent with the findings of Wirth (2012) who noted that a significant number of healthcare practitioners routinely use electronic devices and smartphones which could result in privacy breaches. Research findings that breach incidents involve electronic media are also consistent with Liu et al. (2015) who determined that a significant portion of healthcare data breaches involve information residing on electronic media such as portable computing hardware.

For the type of data privacy breach variable, the analysis showed an estimate value of .193, $p = .000$ indicating that the likely cause of 19% of data privacy breaches is theft or loss. Study findings that the likely cause of data breaches, more often than not, roughly 19% of the time is theft or loss is somewhat contradictory with the research findings of Sen and Borle (2015). Sen and Borle (2015) revealed that loss or theft attributed to the cause of data breaches more frequently than breach occurrences related to malicious intent. Research test results and findings are also inconsistent with Wikina's (2014) test results which revealed that theft represented approximately 47% of breach incidents and about 27% of breaches related to some form of data loss. Study findings could appear to highlight that attackers are changing their attack mechanisms from theft or loss to other forms of attack such as hacking, data destruction, sabotage, or other forms of breach. Additionally, the research findings that roughly 19% of breach incidents involve theft or loss are also are contradictory to the research outcomes reported in the study of Cascardo (2015) who noted that a significant number of HIPAA data breach violations relate to employee theft or unintentional loss.

Although some findings appear to contradict or disconfirm prior research, however, some aspects of the research findings seem to confirm the earlier research results. Liu et al. (2015) determined that criminal behavior, hacking, improper access and disclosure of sensitive information, all causes other than theft or loss, were the underlying cause of most data breaches which appear to confirm study findings that smaller percentage of data breaches approximately 19% involve theft or data loss. Research findings of roughly 19% of data breaches involve theft or loss is indicative that other factors may also likely contribute to data breaches. Findings that possible other factors contribute to data privacy breaches are also consistent with earlier findings of Holtfreter and Harrington (2015) who noted that data breaches relate to three main causes, which include failing to secure and appropriately dispose of sensitive data, theft, or malfeasance committed by non-employees, and external hacking or intrusion attempts. Research findings that factors theft or loss contribute to data breaches about 19% of the time highlighting that other factors contribute to the cause of data breaches, appear to support the findings of Kamoun and Nicho (2014), Kamoun and Nicho (2014) analyzed the root causes of data breaches and found that other causes such as organizational factors, inadequate security defense mechanisms, improper data handling practices, and lack of effective communication and organizational strategies were underlying contributory factors of data security breaches. Kamoun and Nicho (2014) research found that factors other than theft or data loss such as a combination of human errors, lack of appropriately designed technical systems, and inadequate governance, societal, and organizational systems contributed to breach incidents. Findings that the cause of about 19% of data

breaches is theft or loss are also consistent with the findings of Chen et al. (2015) who noted that the source of many organizational data breaches is employee malfeasance or insider threats. Results are also somewhat consistent with the findings of Tu et al. (2015) who highlighted that insider theft or espionage contribute to sources of data loss. Study results also appear to support the research conclusions of Roberts (2014) who noted that a variety of sources can contribute to data privacy breaches including external or insider intrusion of attackers, employee accidental or unintentional data loss, insiders who use valid credentials to abuse, exploit, or steal sensitive data for profit, and disgruntled patients and employees who may target certain systems for damage or disruption.

The selected general loglinear model also showed significant estimate values for nine of the four-way associations or interactions. Table 11 includes parameters estimates for the four-way associations included in the parsimonious model. Using a significance *P*-value of $p < .05$, the analysis resulting from the general loglinear procedure showed that highest significant estimates or odds values among the four-way associations was *[Business Associate Involvement = Yes] * [No. of Individuals Affected = Breach affected 5000 or less individuals] * [Data Storage Location = Electronic data storage location only] * [Type of Data Privacy Breach = Breach cause associated with theft or loss].* Analysis of the highest four-way association represented by an estimate value of slightly larger than one, -1.09, $p = .000$, indicated that according to the model the most common cause of data privacy breaches is theft or loss which results in the exposure of electronically stored data, involving business associates, and affects 5000 or less individuals. However, it is also important to note, that the second highest estimate value

for the four-way association represented by [*Business Associate Involvement = Yes] * [No. of Individuals Affected = Breach Affected 5000 or less individuals] * [Data Storage Location = Electronic data storage location only] * [Type of Data Privacy Breach = Breach cause not associated with theft or loss]* was -.945, $p = .000$. Therefore, it is also important to highlight that 95% of the time, data privacy breaches do not involve business associates but often affect 5000 or less individuals, resulting in exposure of information stored in electronic format. However, study results showed that the underlying cause of the breach incidents does not relate to theft or loss.

Table 11

*Results of General Loglinear Model for Four-Way Associations [Business Associate Involvement] * [No. of Individuals Affected] * [Data Storage Location] * [Type of Data Privacy Breach]*

Parameter estimates	Estimate	Std. error	*Z*	Sig.
[Business associate involvement = yes] * [no. of individuals affected = breach affected 5000 or less individuals] * [data storage location = electronic data storage location only] * [type of data privacy breach = breach cause associated with theft or loss]	-1.099	.206	-5.348	.000*
[Business associate involvement = yes] * [no. of individuals affected = breach affected 5000 or less individuals] * [data storage location = electronic data storage location only] * [type of data privacy breach = breach cause not associated with theft or loss]	-.945	.161	-5.872	.000*
[Business associate involvement = yes] * [no. of individuals affected = breach affected 5000 or less individuals] * [data storage location = combination of physical, electronic, or other data storage location only] * [type of data privacy breach = breach cause associated with theft or loss]	-.361	.158	-2.282	.022*
[Business associate involvement = yes] * [no. of individuals affected = breach affected 5000 or less individuals] * [data storage location = combination of physical, electronic, or other data storage location only] * [type of data privacy breach = Breach cause not associated with theft or loss]	-.319	.121	-2.631	.009*
[Business associate involvement = yes] * [no. of individuals affected = breach affected more than individuals] * [data storage location = electronic data storage location only] * [type of data privacy breach = breach cause associated with theft or loss]	-.254	.167	-1.517	.129

(table continues)

Parameter estimates	Estimate	Std. error	*Z*	Sig.
[Business associate involvement = yes] * [no. of Individuals affected = breach affected more than individuals] * [data storage location = electronic data storage location only] * [type of data privacy breach = breach cause not associated with theft or loss]	-.341	.137	-2.492	.013*
[Business associate involvement = yes] * [no. of individuals affected = breach affected more than individuals] * [data storage location = combination of physical, electronic, or other data storage location only] * [type of data privacy breach = breach cause associated with theft or loss]	.342	.129	2.644	.008*
[Business Associate Involvement = no] * [no. of Individuals Affected = Breach affected 5000 or less individuals] * [data Storage location = electronic data storage location only] * [type of data privacy breach = breach cause associated with theft or loss]	-.239	.131	-1.818	.069
[Business associate involvement = no] * [no. of individuals affected = breach affected 5000 or less individuals] * [data storage location = electronic data storage location only] * [type of data privacy breach = breach cause not associated with theft or loss]	-.353	.082	-4.328	.000*
[Business associate involvement = no] * [no. of Individuals affected = breach affected 5000 or less individuals] * [data storage location = combination of physical, electronic, or other data storage location only] * [type of data privacy breach = breach cause associated with theft or loss]	.204	.083	2.459	.014*
[Business associate involvement = no] * [no. of individuals affected = breach affected more than individuals] * [data storage location = electronic data storage location only] * [type of data privacy breach = breach cause associated with theft or loss]	.236	.091	2.599	.009*

Note. *Significant at the $p < 0.05$ level. Sig. = *p*-value

Integrated system theory was the theoretical framework used in this study. Integrated system theory is an appropriate framework for understanding information security outcomes, strategies, and organizational practices (Sharma & Sugumaran, 2011). The framework of integrated system theory consists of aspects of security policy, risk management, auditing, and internal controls monitoring, which business leaders can use to effectively manage various information security issues (Järveläinen, 2012). In terms of the underlying theoretical connections, the research showed that about 19% of the time data breaches electronic media. Findings from the study also showed that healthcare

providers contribute to roughly 74% of data breaches and approximately 19% of the breaches relate to theft or loss. In order to reduce future data security incidents, drawing from the theory, it appears that organizational leaders could adopt certain underlying aspects of integrated system theory in their organizations to reduce future security incidents. For example, aspects of the framework such as implementation of formal information security policies, auditing, and effective internal controls monitoring could to help reduce the likelihood and odds of future privacy incidents. Integrated system theory relate to aspects of managerial planning, oversight, governance, contingency management, and control (Hong et al., 2003). In terms of managerial planning, oversight, and control healthcare providers could analyze decisions relating to data storage and determine for example if healthcare data should be stored in physical, electronic, or other forms in order to reduce the odds of data breach and minimize the number of individuals potentially affected by data privacy breaches.

Applications to Professional Practice

Aspects of the research findings could apply to professional practice, and both managers and business leaders might utilize the results of the study to minimize the security risks. The research results showed that for data breach incidents, it is 1.044 more times likely than not, that security breaches will affect up to 5000 individuals. Applying study results to professional practice might reveal that in the future, to possibly reduce the number of individuals affected by a breach incident, business leaders of healthcare entities should limit the amount of personal information they collect and store. Medical data contains some of the most confidential or otherwise personal and sensitive

information about an individual (Kamoun & Nicho, 2014). Managers might consider reducing the number of electronic computing devices such laptops, mobile phones, and other portable devices that transmit, process, or store sensitive personal information thereby reducing the potential and risk of unwanted exposure. Additionally, healthcare leaders might consider minimally collecting and storing only critical or essential elements of personal information relating to individual health records and consider refraining from overly collecting sensitive and confidential information. Restricting the collection of personal and sensitive health data to only certain essential records could minimize exposure risks and potentially reduce the number individuals affected when security breaches occur. Business leaders might consider maintaining and managing sensitive health information on an as needed one-time basis only to prevent future exposure of breached data.

Results of the study showed that about 74% of data breaches involve healthcare providers and non-healthcare providers such as health plans or clearinghouses are generally not involved in the majority of security breaches and these research results could be applicable to professional practice. Study findings appear to highlight that among covered entities, healthcare providers need to strengthen security prevention efforts or possibly invest in preventative security measures. The threat landscape and the nature of security incidents are constantly changing (Chaudhary & Lucas, 2014). Although study findings revealed that business associates were not involved in security the 95% of data breaches. In terms of professional practices, in order to continue to lessen the impact of data breaches caused by business associates and external partners,

healthcare leaders may need to continue to forge effective partnerships and relationships resulting in reduced risks. However, healthcare managers might also need to evaluate, examine, and assess the security infrastructure and controls within their businesses and the evidence appear to suggest that data breaches originate within healthcare entities rather than originate with external entities, business associates or third-party vendors.

Implications for Social Change

Organizational leaders have a legal duty and regulatory obligation to prevent data breaches and protect personal information (Tu et al., 2015). A critical step in preventing data breaches in healthcare is for organizational leaders to identify threats that lead to data loss (Tu et al., 2015). Communication, information sharing, and collaboration among public and private security leaders is a fundamental component of an effective risk management strategy and information security program (Borum, Felker, Kern, Dennesen, & Feyes, 2015). Research findings from this study may contribute to increased interest, dialogue, discussion, and collaboration among public and private security leaders about risk management and information security strategies resulting in societal and organizational impacts that can lead to positive social change. Additionally, security leaders often measure the success of their organization in terms of security awareness and training of end-users, quality of the workforce, incident response times, percentage of downtime, or by assessing the number of policy violations and security breach incidents (Borum et al., 2015). Security leaders might utilize the results of this study as a measurement tool to assess and compare data breach incidents within their entities to determine if trends found in this study are applicable to their perspective organizations.

Fraudulent claims and overall healthcare fraud resulting from data breaches can affect patient safety, contribute to errors in diagnosis and treatment, or result in denial of critical patient services (Gray et al., 2013). Research results from this study may provide managers with a broader understanding of information pertaining to data breaches so that business leaders might design, implement, and adopt information security policies, procedures, and controls that are less susceptible to threats and potential exploits thereby increasing overall patient safety and minimizing disruptions and errors which could result from fraudualent claims and healthcare fraud. Advances in healthcare information systems can lead to improvements in healthcare and reduced medical costs (Shin, Jeon, Ju, Lee, & Jeong, 2015). Findings from this study might equip managers with the skills they need to understand aspects of data privacy breaches in order to create effective healthcare information systems that reduce medical costs and can lead to improvements in healthcare.

Additionally, study findings revealed information relating to privacy breaches that healthcare professionals and security organizational leaders could employ to prevent future data privacy breaches issues leading to more positive measures of organizational success. Regardless of the complexities and safeguards implemented within organizational systems, perpetrators will continually find means of to target systems for breach, exploit, and attack (Baskerville, Hee Park, & Kim, 2014). Business leaders may utilize the findings and recommendations from this study to obtain an understanding of healthcare data breaches in order to continually improve organizational systems which may decrease the likelihood that systems are targeted, exploited, or attacked which

reduces the potential of data loss and unwanted exposure of consumer information. Ultimately, data breaches of healthcare information can have both economic and financial implications (Hayhurst, 2014). Security practitioners, managers, and healthcare leaders may utilize the findings from this study to improve security within their organizations which could minimize the business and financial impacts of data breaches generally associated with fines, noncompliance, legal risks, and other penalties. Findings from this study could also equip industry managers and business leaders with the information they need to minimize the economic and societal impacts of medical fraud, identity theft, or financial fraud that could occur when healthcare entities expose, exploit, and breach sensitive, personal, or confidential information.

Recommendations for Action

Security professionals, healthcare leaders, and other individuals responsible for securing and managing sensitive or confidential healthcare information may find the results of this study relevant and useful. Additionally, information and research findings from this study may be appropriate for seminars, conferences, and tradeshows geared towards helping organizations strengthen and protect information security practices and programs. This study revealed a number of findings resulting in possible managerial recommendations that security professionals and healthcare leaders may find relevant. The study results showed that over 70% of data privacy breaches involve healthcare providers. Healthcare data is sensitive and may contain confidential, personal, or otherwise private information about patients and individuals (Shin et al., 2015). Additionally, data breaches can have a devastating financial impact on firms and

penalties for failing to comply with laws and regulations may vary (Zelle & Whitehead, 2014). Thus, a possible approach data leaders of healthcare providers might employ to reduce future data breaches is to identify and streamline the number of devices that store sensitive data. Organizations can restrict the storage and copying of personal data to non-encrypted portable devices (Tu et al., 2015). Restricting the number of devices that store sensitive data could result in less sensitive information available for attack which in essence could reduce societal risks and limit potential harm and damages to consumers and individuals resulting from unwanted data loss. Next, the findings also showed that over 95% of data breaches do not involve business associates or external third party vendors. The findings from this study appear to highlight that since security breaches are not associated with data managed and maintained by external vendors, then security incidents may likely result from data maintained and stored internally within healthcare entities. Therefore, in order to minimize societal impacts of data breaches managers might consider implementing robust automatic threat monitoring and detection programs to identify security threats before data breaches occur. In order to prevent unauthorized data loss, managers can deploy endpoint security solutions to monitor data regularly and routinely identify policy violations (Tu et al., 2015).

Finally, data breaches and exposure of sensitive information such as (a) names, (b) contact information, (c) passwords, (d) social security numbers, (e) banking and financial related information, (f) credit card numbers, or (g) other personal identifying information could result in fraud or identity theft (Holtfreter & Harrington, 2015). Even the most sophisticated and robust systems are susceptible to exploitation and attack

(Smyth, 2014). However, security is more effective when organizations establish and implement formal information security programs (Smyth, 2014). Study findings revealed that about 19% of the time the source or likely cause of data breaches relates to theft or data loss. Thus, from the research findings, it would appear that since theft or data loss contribute to less than 20% of data breaches the cause of the remainder of security breaches likely relate to a myriad of other factors. Varying causes of data breaches could mean that organizational security measures are inadequate, ineffective, or somehow limited and not sufficiently designed to protect against threats. Therefore, in order to minimize the potential for fraud or identity theft that could occur when organizations expose sensitive and confidential healthcare data, security professionals, and business managers might consider evaluating existing security programs, controls, procedures, and weaknesses within their companies to identify potential gaps that could lead to future threats or exploitation. Business leaders might consider evaluating existing processes in order to find effective solutions and consider re-designing information security programs to improve overall performance. Attackers often utilize digital technologies and electronic means to commit attacks such as identity theft, espionage, system malfunctions, and data destruction which could result information security breaches, or data exploitation (Smyth, 2014). Research findings showed that the underlying cause of data breaches relate to factors beyond theft and data loss. Therefore, in order to improve and increase the effectiveness of information security and prevention programs within their organizations, healthcare practitioners, and security leaders may utilize study results

to examine technology strategies, information security risks, and potential threats that could contribute to other causes data privacy breaches.

Recommendations for Further Study

This study did not include an examination and analysis of all healthcare data breaches that occurred within the United States as data breaches and threats continue to evolve. Therefore, future researchers might find it useful to analyze other sources of data breach information related to other industries such as financial, telecommunications, governmental, or educational sectors to determine whether the study results are applicable, consistent, and similar across other industries. Next, the focus of this study was healthcare security breaches of covered entities that affected 500 or more individuals. Scholars may find it beneficial to examine security breaches of healthcare entities that affected fewer than 500 individuals to compare the findings of this study to determine if there is relevant information business leaders across the healthcare sector may find useful. This research related to an examination of data privacy breaches of healthcare entities affected by the U.S. healthcare laws, however future studies with a focus on non-covered entities that manage aspects of healthcare data may also be beneficial to security professionals and organizational leaders. Future scholars may find it useful to examine the challenges of non-covered entities to determine if there are unique nuisances and intricacies that healthcare security professionals and leaders of covered entities might need to be aware of when managing and securing confidential and sensitive patient data.

The focus of this study was on the association of data privacy breaches, business associates, covered entities, the number of individual affected, and data storage locations. However, in order to minimize future business and consumer threats, leaders may find it relevant to understand the underlying nature of security breaches in terms of why and how data breaches occur and may need to understand how organizational, environmental, or other factors might contribute to information security weakness and threats which may have an impact on data breaches. Information contained in this study related to U.S. healthcare institutions covered under HITECH and HIPAA laws. An examination of healthcare security breaches that occurred within countries outside of the U.S. might yield relevant information for security managers and healthcare professionals. Future research devoted to fully understanding the risk profile and security posture of healthcare providers might be relevant in order help medical practitioners better understand why data breaches appear to involve healthcare providers over 70% of the time rather than involve other types of healthcare entities. Scholarly inquiry devoted to understanding the unique challenges of healthcare providers specifically relative to data privacy breaches may help to prevent future security issues. Finally, the data source used in this study was the DHHS OCR online breach database. However, possible future research may also include analyzing other databases and repositories of breach information maintained by other entities and governmental agencies to potentially identify findings or other opportunities to improve business practice.

Reflections

This study involved examining a secondary data source to understand associations among variables related to data privacy breaches. Preparation and coding of the data set involved utilizing different features and syntax available in SPSS. In some instances, I had to utilize available resources to learn and acquire new SPSS data analytical skills and in other cases, I had to update or refresh existing skills as I worked through preparing and analyzing the data and study results. At the beginning of the research process, I thought I had a broad understanding of information security threats. However, during the research process, I learned to appreciate varying perspectives and multiple views that in some cases were different from my own internal perspectives. Additionally, during the research journey, I realized that scholars have a certain level of inherent internal biases and preconceptions when conducting their work. However, I learned through the research process that acknowledging inner biases exist allowed me to remain transparent, open, and objective when I conducted the study and examined resulting findings. The research process enabled me to gain some new insights into how to approach and solve problems. I have also forged some new found friendships with many of my colleagues along this journey. Finally, utilizing a secondary data source for this study gave me a new appreciation of the many sources of existing yet relevant and useful that are available to researchers. I plan to continue to leverage and utilize existing sources of relevant information to find solutions to real-world business problems, discover new ideas, and extend the body of information security research.

Summary and Study Conclusions

Data privacy breaches can result in financial fraud, identity theft, reputational damage, and might lead to regulatory risks associated with fines, legal challenges , and other penalties for non-compliance with healthcare rules. Security incidents involving healthcare information might result in fraudulent submission of medical claims, healthcare billing and insurance fraud, improper diagnosis and treatment resulting from erroneous or inaccurate information, or exposure of sensitive patient medical records. Additionally, costs associated with breach mitigation and incident response might hinder an organization's long-term financial viability. Therefore, safeguarding personal, confidential; and sensitive healthcare information will likely rise to the level of strategic priority for security practitioners and business leaders.

There may be operational benefits and cost savings realized when organizations automate and digitize healthcare data, yet, security threats, exploits, and attack mechanisms will likely remain. Research findings showed that healthcare providers are the likely source of data privacy breaches and that breach data often consists of electronic records other forms of digital information. In terms of the underlying cause of security breach incidents, results revealed that the threat landscape is continuously evolving and appear to indicate that a myriad of factors other than data loss and theft contribute unwanted exposure and breaches of healthcare data. Therefore, in order to effectively manage information security and minimize possible societal, financial, and reputational damage resulting from security incidents and data breaches, managers should examine, assess, evaluate, and continuously monitor existing information security programs and

employ appropriate preventative measures that reduce the impact of data privacy breaches and other information security risks.

References

Abu-Musa, A. (2010). Information security governance in Saudi organizations: An empirical study. *Information Management & Computer Security*, *18*, 226–276. doi:10.1108/09685221011079180

Adebayo, A. O. (2012). A foundation for breach data analysis. *Journal of Information Engineering and Applications*, *2*(4), 17–23. Retrieved from http://www.iiste.org/Journals/index.php/JIEA

Adler, J., Demicco, M., & Neiditz, J. (2015). Critical privacy and data security risk management issues for the franchisor. *Franchise Law Journal*, *35*, 79–92. Retrieved from http://www.americanbar.org/

Ahuja, S. P., & Rolli, A. C. (2012). Exploring the convergence of mobile computing with cloud computing. *Network and Communication Technologies*, *1*(1), 97–102. doi:10.5539/nct.v1n1p97

Ajithkumar, K. (2012). Medical research: How to formulate a research question? *Kerala Journal of Orthopaedics*, *25*, 47–49. Retrieved from www.kjoonline.org

Al-Abdallah, G. M. (2015). The impact of Internet marketing research on achieving competitive advantage. *International Journal of Arts & Sciences*, *8*, 619–627. Retrieved from http://www.josa.ro

Alvesson, M., & Sandberg, J. (2011). Generating research questions through problematization. *Academy of Management Review*, *36*, 247–271. doi:10.5465/amr.2011.59330882

Amundson, E. P., & Cole, J. (2013). Dakotacare update: What is a business associate agreement? HIPAA Omnibus Rule-Privacy and security changes. *South Dakota Medicine: The Journal of the South Dakota State Medical Association*, *66*, 432–433. Retrieved from https://www.sdsma.org/

Anandarajan, M., D'Ovidio, R., & Jenkins, A. (2013). Safeguarding consumers against identity-related fraud: Examining data breach notification legislation through the lens of routine activities theory. *International Data Privacy Law*, *3*, 51–60. doi:10.1093/idpl/ips035

Anderson, K. M., & Paterson, M. (2015). Overview of secondary data analysis with a description of heart failure hospitalizations from the national hospital discharge survey. *Clinical Scholars Review*, *8*, 130–138. doi:10.1891/1939-2095.8.1.130

Appari, A., & Johnson, M. E. (2010). Information security and privacy in healthcare: Current state of research. *International Journal of Internet and Enterprise Management*, *6*, 279–314. doi:10.1504/ijiem.2010.035624

Arghode, V. (2012). Qualitative and quantitative research: Paradigmatic differences. *Global Education Journal*, *2012*(4), 155–163. Retrieved from http://franklinpublishing.net/globaleducation.html

Arora, S., Yttri, J., & Nilsen, W. (2014). Privacy and security in mobile health mHealth research. *Alcohol Research: Current Reviews*, *36*(1), 143–150. Retrieved from http://www.arcr.niaaa.nih.gov/

Avasthi, A., Ghosh, A., Sarkar, S., & Grover, S. (2013). Ethics in medical research: General principles with special reference to psychiatry research. *Indian Journal of Psychiatry*, *55*(1), 86–91. doi:10.4103/0019-5545.105525

Ayyagari, R. (2012). An exploratory analysis of data breaches from 2005-2011: Trends and insights. *Journal of Information Privacy & Security*, *8*, 33–56. doi:10.1080/15536548.2012.10845654

Badara, M. S., & Saidin, S. Z. (2014). Internal audit effectiveness: Data screening and preliminary analysis. *Asian Social Science*, *10*(10), 76–85. doi:10.5539/ass.v10n10p76

Baker, R., Brick, J. M., Bates, N. A., Battaglia, M., Couper, M. P., Dever, J. A., … Tourangeau, R. (2013). Summary report of the Aapor task force on non-probability sampling. *Journal of Survey Statistics and Methodology*, *1*, 90–143. doi:10.1093/jssam/smt008

Baskerville, R., Hee Park, E., & Kim, J. (2014). An emote opportunity model of computer abuse. *Information Technology & People*, *27*, 155–181. doi:10.1108/itp-11-2011-0068

Berezina, K., Cobanoglu, C., Miller, B. L., & Kwansa, F. A. (2012). The impact of information security breach on hotel guest perception of service quality, satisfaction, revisit intentions and word-of-mouth. *International Journal of Contemporary Hospitality Management*, *24*, 991–1010. doi:10.1108/09596111211258883

Bettany-Saltikov, J., & Whittaker, V. J. (2014). Selecting the most appropriate inferential statistical test for your quantitative research study. *Journal of Clinical Nursing*, *23*, 1520–1531. doi:10.1111/jocn.12343

Birchall, J. (2014). Qualitative inquiry as a method to extract personal narratives: Approach to research into organizational climate change mitigation. *The Qualitative Report*, *19*, 1–18. Retrieved from http://tqr.nova.edu/

Blee, K. M., & Currier, A. (2011). Ethics beyond the IRB: An introductory essay. *Qualitative Sociology*, *34*, 401–413. doi:10.1007/s11133-011-9195-z

Boo, S., & Froelicher, E. S. (2013). Secondary analysis of national survey datasets. *Japan Journal of Nursing Science*, *10*, 130–135. doi:10.1111/j.1742-7924.2012.00213.x

Borum, R., Felker, J., Kern, S., Dennesen, K., & Feyes, T. (2015). Strategic cyber intelligence. *Information and Computer Security*, *23*, 317–332. doi:10.1108/ics-09-2014-0064

Bose, I., & Leung, A. C. M. (2014). Do phishing alerts impact global corporations? A firm value analysis. *Decision Support Systems*, *64*, 67–78. doi:10.1016/j.dss.2014.04.006

Bradt, J., Burns, D. S., & Creswell, J. W. (2013). Mixed methods research in music therapy research. *Journal of Music Therapy*, *50*, 123–48. doi:10.1093/jmt/50.2.123

Brakewood, B., & Poldrack, R. A. (2013). The ethics of secondary data analysis: Considering the application of Belmont principles to the sharing of neuroimaging data. *NeuroImage*, *82*, 671–676. doi:10.1016/j.neuroimage.2013.02.040

Breaux, R. W., Black, E. W., & Newman, T. (2014). A guide to data protection and breach response: Part 1. *Intellectual Property & Technology Law Journal*, *26*(7), 3–10. Retrieved from http://www.aspenpublishers.com

Bredfeldt, C. E., Butani, A. L., Pardee, R., Hitz, P., Padmanabhan, S., & Saylor, G. (2013). Managing personal health information in distributed research network environments. *BMC Medical Informatics & Decision Making*, *13*(1), 116–122. doi:10.1186/1472-6947-13-116

Brezina, P. R., Vlahos, N. F., Lai, T.-H., Garcia, J. E., Wallach, E. E., & Zhao, Y. (2012). The impact of luteal phase support on endometrial estrogen and progesterone receptor expression: A randomized control trial. *Reproductive Biology and Endocrinology*, *10*, 991–1010. doi:10.1186/1477-7827-10-16

Brughelli, M., Cronin, J., Levin, G., & Chaouachi, A. (2008). Understanding change of direction ability in sport: A review of resistance training studies. *Sports Medicine*, *38*, 1045–1063. doi:10.2165/00007256-200838120-00007

Bulpitt, H., & Martin, P. (2010). Who am I and what am I doing? Becoming a qualitative research interviewer. *Nurse Researcher*, *17*(3), 7–16. doi:10.7748/nr2010.04.17.3.7.c7741

Callahan, J. L. (2014). Writing literature reviews a reprise and update. *Human Resource Development Review*, *13*, 271–275. doi:10.1177/1534484314536705

Carcary, M. (2013). IT risk management: A capability maturity model perspective. *Electronic Journal of Information Systems Evaluation*, *16*, 1–13. Retrieved from http://www.ejise.com/

Cascardo, D. (2012). What to do before the Office for Civil Rights comes knocking: Part I. *The Journal of Medical Practice Management: MPM*, *27*, 337–340. Retrieved from http://www.mpmnetwork.com

Cascardo, D. (2013). HIPAA security standards: Getting ready for prime time. *The Journal of Medical Practice Management: MPM*, *29*, 24–28. Retrieved from http://www.mpmnetwork.com

Cascardo, D. (2014). HIPAA investigation risks are increasing: Make sure you avoid the wall of shame. *The Journal of Medical Practice Management: MPM*, *30*, 119–123. Retrieved from http://www.mpmnetwork.com

Cascardo, D. (2015). Physician challenges in 2015. *The Journal of Medical Practice Management: MPM*, *30*, 395–398. Retrieved from http://www.mpmnetwork.com

Chang, D., Han, X., & Chen, B. (2014). Research on construction and application of individual knowledge management maturity evaluation model. *Journal of Computing & Information Technology*, *22*(LISS 2013), 53–61. doi:10.2498/cit.1002274

Chang, K.-C., & Wang, C.-P. (2011). Information systems resources and information security. *Information Systems Frontiers*, *13*, 579–593. doi:10.1007/s10796-010-9232-6

Chaudhary, R., & Lucas, M. (2014). Privacy risk management. *Internal Auditor*, *71*(5), 37–40. Retrieved from http://www.theiia.org/intauditor/

Cheng, H. G., & Phillips, M. R. (2014). Secondary analysis of existing data: Opportunities and implementation. *Shanghai Archives of Psychiatry*, *26*, 371–375. doi:10.11919/j.issn.1002-0829.214171

Chen, J. V., Li, H.-C., Yen, D. C., & Bata, K. V. (2012). Did IT consulting firms gain when their clients were breached? *Computers in Human Behavior*, *28*, 456–464. doi:10.1016/j.chb.2011.10.017

Chen, X., Bose, I., Leung, A. C. M., & Guo, C. (2011). Assessing the severity of phishing attacks: A hybrid data mining approach. *Decision Support Systems*, *50*, 662–672. doi:10.1016/j.dss.2010.08.020

Chen, Y., Ramamurthy, K. R., & Wen, K.-W. (2015). Impacts of comprehensive information security programs on information security culture. *The Journal of Computer Information Systems*, *55*, 11–19. Retrieved from http://www.iacis.org/jcis/jcis.php

Christenson, B., Delong-Hamilton, T., Panos, P., Krase, K., Buchan, V., Farrel, D., … Buchan, V. (2015). Evaluating social work education outcomes: The SWEAP field practicum placement assessment instrument (FPPAI). *Field Educator*, *5*(1), 1–13. Retrieved from http://fieldeducator.simmons.edu

Çilan, A. Ç. (2014). Latent class analysis for measuring Turkish people's future expectations for Turkey. *Journal of Applied Statistics*, *41*, 519–529. doi:10.1080/02664763.2013.842961

Clarke, D. R., Breen, L. S., Jacobs, M. L., Franklin, R. C. G., Tobota, Z., Maruszewski, B., & Jacobs, J. P. (2008). Verification of data in congenital cardiac surgery. *Cardiology in the Young*, *18*, 177–187. doi:10.1017/s1047951108002862

Clark, L. W., & Bilimoria, N. M. (2013). How HIPAA final rules affect health information technology vendors. *The Journal of Medical Practice Management: MPM*, *29*, 56–58. Retrieved from http://www.mpmnetwork.com

Classen, H. W., Fogarty, M., & Mier, B. (2012). Anatomy of a business associate agreement, Part I. *Journal of Health Care Compliance*, *14*(4), 5–28, 69–73. Retrieved from http://www.wklawbusiness.com

Claunch, D., & McMillan, M. (2013). Determining the right level for your IT security investment. *Healthcare Financial Management*, *67*(5), 100–103. Retrieved from https://www.hfma.org/hfm

Coronado, A. J., & Wong, T. L. (2014). Healthcare cybersecurity risk management: Keys to an effective plan. *Biomedical Instrumentation & Technology*, *48*, 26–30. doi:10.2345/0899-8205-48.s1.26

Cramon, P., Rasmussen, Å. K., Bonnema, S. J., Bjorner, J. B., Feldt-Rasmussen, U., Groenvold, M., … Watt, T. (2014). Development and implementation of progmatic: A clinical trial management system for pragmatic multi-centre trials, optimised for electronic data capture and patient-reported outcomes. *Clinical Trials*, *11*, 344–354. doi:10.1177/1740774513517778

Cucoranu, I. C., Parwani, A. V., West, A. J., Romero-Lauro, G., Nauman, K., Carter, A. B., … Pantanowitz, L. (2013). Privacy and security of patient data in the

pathology laboratory. *Journal of Pathology Informatics*, *4*, 23–39. doi:10.4103/2153-3539.108542

Das, S., Mukhopadhyay, A., & Anand, M. (2012). Stock market response to information security breach: A study using firm and attack characteristics. *Journal of Information Privacy & Security (Ivy League Publishing)*, *8*, 27–55. doi:10.1080/15536548.2012.10845665

Dean, J. (2014). Personal protective equipment: An antecedant to safe behavior. *Professional Safety*, *59*(2), 41–46. Retrieved from http://www.asse.org/professional-safety/

DeCarlo, T. E., Laczniak, R. N., Azevedo, K. A., & Ramaswami, S. N. (2000). On the log-linear analysis of multiple response data. *Marketing Letters*, *11*, 349–361. doi:10.1023/A:1008189229857

Dehner, C., Schick, S., Hell, W., Richter, P., Kraus, M., & Kramer, M. (2013). In-vivo kinematics of the cervical spine in frontal sled tests. *Global Journal of Health Science*, *5*(3), 115–126. doi:10.5539/gjhs.v5n3p115

Demment, M. M., Haas, J. D., & Olson, C. M. (2014). Changes in family income status and the development of overweight and obesity from 2 to 15 years: A longitudinal study. *BMC Public Health*, *14*, 1–9. doi:10.1186/1471-2458-14-417

Dhar, T., & Weinberg, C. B. (2015). Measurement of interactions in non-linear marketing models: The effect of critics ratings and consumer sentiment on movie demand. *International Journal of Research in Marketing*, 1–17. doi:10.1016/j.ijresmar.2015.10.003

Diepen, M. van, Schroijen, M. A., Dekkers, O. M., Rotmans, J. I., Krediet, R. T., Boeschoten, E. W., & Dekker, F. W. (2014). Predicting mortality in patients with diabetes starting dialysis: e89744. *PLoS One*, *9*(3), 1–7. doi:10.1371/journal.pone.0089744

Din, G. Y., Zugman, Z., & Khashper, A. (2014). Utilization of primary and secondary medical care among disadvantaged populations: A log-linear model analysis. *Global Journal of Health Science*, *6*(5), 9–21. doi:10.5539/gjhs.v6n5p9

Duxbury, T. (2012). Towards more case study research in entrepreneurship. *Technology Innovation Management Review*, *2*(3), 9–17. Retrieved from http://timreview.ca

Dzazali, S., & Zolait, A. H. (2012). Assessment of information security maturity: An exploration study of Malaysian public service organizations. *Journal of Systems and Information Technology*, *14*(1), 23–57. doi:10.1108/13287261211221128

Ellis, T. J., & Levy, Y. (2009). Towards a guide for novice researchers on research methodology: Review and proposed methods. *Issues in Informing Science & Information Technology*, *6*, 323–337. Retrieved from http://www.informingscience.org

Espinosa, M. M., Bieski, I. G. C., & Martins, D. T. de O. (2012). Probability sampling design in ethnobotanical surveys of medicinal plants. *Revista Brasileira de Farmacognosia*, *22*, 1362–1367. doi:10.1590/s0102-695x2012005000091

Farrelly, P. (2013). Choosing the right method for a qualitative study. *British Journal of School Nursing*, *8*, 93–95. doi:10.12968/bjsn.2013.8.2.93

Fernandes, A. C., Cloete, D., Broadbent, M. T., Hayes, R. D., Chang, C.-K., Jackson, R. G., … Callard, F. (2013). Development and evaluation of a de-identification procedure for a case register sourced from mental health electronic records. *BMC Medical Informatics and Decision Making*, *13*(71). doi:10.1186/1472-6947-13-71

Fetters, M. D., Curry, L. A., & Creswell, J. W. (2013). Achieving integration in mixed methods designs-principles and practices. *Health Services Research*, *48*, 2134–2156. doi:10.1111/1475-6773.12117

Filbeck, G., Swinarski, M., & Zhao, X. (2013). Shareholder reaction to firm investments in the capability maturity model: An event study. *European Journal of Information Systems*, *22*, 170–190. doi:10.1057/ejis.2012.54

Flaherty, J. L. (2014). Digital diagnosis: Privacy and the regulation of mobile phone health applications. *American Journal of Law and Medicine*, *40*, 416–441. Retrieved from http://www.aslme.org/

Fouka, G., & Mantzorou, M. (2011). What are the major ethical issues in conducting research? Is there a conflict between the research ethics and the nature of nursing? *Health Science Journal*, *5*, 3–14. Retrieved from http://www.hsj.gr

Fraser, M. (2015). Reflections on the process of conducting secondary analysis of qualitative data concerning informed choice for young people with a disability in transitions. *Forum: Qualitative Social Research*, *16*(3). Retrieved from http://www.qualitative-research.net/index.php/fqs

Fujii, L. A. (2012). Research ethics 101: Dilemmas and responsibilities. *PS, Political Science & Politics*, *45*, 717–723. doi:10.1017/s1049096512000819

Fu, K. (2014). A contrastive survey of speech acts in Hong Kong bilingual legislative texts: A case study of CO and SPR. *English Language Teaching*, *7*(5), 102–109. doi:10.5539/elt.v7n5p102

Fusch, P. I., & Ness, L. R. (2015). Are we there yet? Data saturation in qualitative research. *The Qualitative Report*, *20*, 1408–1416. Retrieved from http://tqr.nova.edu/

Gambrel, L. E., & Butler, J. L. (2013). Mixed methods research in marriage and family therapy: A content analysis. *Journal of Marital & Family Therapy*, *39*, 163–181. doi:10.1111/j.1752-0606.2011.00260.x

Gasch, A. (2012). Ten tips for successful electronic health records deployment. *The Journal of Medical Practice Management: MPM*, *28*(3), 210–213. Retrieved from http://www.mpmnetwork.com

Gatzlaff, K. M., & McCullough, K. A. (2012). Implications of privacy breaches for insurers. *Journal of Insurance Regulation*, *31*, 197–216. Retrieved from http://www.naic.org/

Goldstein, M. M. (2014). Health information privacy and health information technology in the US correctional setting. *American Journal of Public Health*, *104*, 803–809. doi:10.1001/jama.2015.2252

Gomes, A., Saha, A., Datta, P., & Gomes, A. (2013). Research ethics for young researchers. *Indian Journal of Pharmacology*, *45*, 540–541. doi:10.4103/0253-7613.117775

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). Externalities and the magnitude of cyber security underinvestment by private sector firms: A modification of the Gordon-Loeb model. *Journal of Information Security*, *6*, 24–30. doi:10.4236/jis.2015.61003

Graves, C., & Rutherford, S. (2012). Writing a scientific research testable question: The first step in using online data sets for guided inquiry assignments. *Journal of College Science Teaching*, *41*, 46–51. Retrieved from http://www.nsta.org/college/

Gray, D., Citron, D. K., & Rinehart, L. C. (2013). Fighting cybercrime after United States V. Jones. *Journal of Criminal Law & Criminology*, *103*, 745–801. Retrieved from http://www.law.northwestern.edu/jclc/

Green, H. E. (2014). Use of theoretical and conceptual frameworks in qualitative research. *Nurse Researcher*, *21*(6), 34–38. doi:10.7748/nr.21.6.34.e1252

Grzybek, M. J., Bajer, A., Bednarska, M., Al-Sarraf, M., Behnke-Borowczyk, J., Harris, P. D., … Behnke, J. M. (2015). Long-term spatiotemporal stability and dynamic changes in helminth infracommunities of bank voles (Myodes glareolus) in NE Poland. *Parasitology*, *142*, 1722–1743. doi:10.1017/S0031182015001225.

Haley, C. B., Laney, R. C., Moffett, J. D., & Nuseibeh, B. (2006). Using trust assumptions with security requirements. *Requirements Engineering*, *11*, 138–151. doi:10.1007/s00766-005-0023-4

Hanson-Abromeit, D., & Moore, K. S. (2014). The systematic review as a research process in music therapy. *Journal of Music Therapy*, *51*, 4–38. doi:10.1093/jmt/thu002

Haque, M. M., Chin, H. C., & Debnath, A. K. (2012). An investigation on multi-vehicle motorcycle crashes using log-linear models. *Safety Science*, *50*, 352–362. doi:10.1016/j.ssci.2011.09.015

Haveman, H. A., Habinek, J., & Goodman, L. A. (2012). How entrepreneurship evolves: The founders of new magazines in America, 1741–1860. *Administrative Science Quarterly*, *57*, 585–624. doi:10.1177/0001839212467168

Hayden, J. R. (2013). Health plans and HIPAA privacy and security. *Journal of Health Care Compliance*, *15*(2), 45–59. Retrieved from http://www.wklawbusiness.com

Hayhurst, C. (2014). Is your patient data secure? *Biomedical Instrumentation & Technology*, *48*, 166–173. doi:10.2345/0899-8205-48.3.166

Hedström, K., Karlsson, F., & Kolkowska, E. (2013). Social action theory for understanding information security non-compliance in hospitals: The importance of user rationale. *Information Management & Computer Security*, *21*, 266–287. doi:10.1108/imcs-08-2012-0043

Henderson, L. S., & Stackman, R. W. (2010). An exploratory study of gender in project management: Interrelationships with role, location, technology, and project cost. *Project Management Journal*, *41*(5), 37–55. doi:10.1002/pmj.20175

Henderson, L. S., Stackman, R. W., & Koh, C. Y. (2013). Women project managers: The exploration of their job challenges and issue selling behaviors. *International*

Journal of Managing Projects in Business, *6*, 761–791. doi:10.1108/IJMPB-06-2012-0033

Heyvaert, M., Maes, B., & Onghena, P. (2013). Mixed methods research synthesis: Definition, framework, and potential. *Quality & Quantity*, *47*, 659–676. doi:10.1007/s11135-011-9538-6

Holosko, M. J., Jolivette, K., & Houchins, D. E. (2014). Reporting guidelines for intervention and evaluation research conducted in juvenile and adult corrections: A guide for better quality and uniform standardization. *Journal of Correctional Education*, *65*(3), 66–89. Retrieved from https://www.ashland.edu/founders/programs/correctional-education/journal-correctional-education

Holtfreter, R. E., & Harrington, A. (2015). Data breach trends in the United States. *Journal of Financial Crime*, *22*, 242–260. doi:10.1108/jfc-09-2013-0055

Hong, K.-S., Chi, Y.-P., Chao, L. R., & Tang, J.-H. (2003). An integrated system theory of information security management. *Information Management & Computer Security*, *11*, 243–248. doi:10.1108/09685220310500153

Hong, K.-S., Chi, Y.-P., Chao, L. R., & Tang, J.-H. (2006). An empirical study of information security policy on information security elevation in Taiwan. *Information Management & Computer Security*, *14*, 104–115. doi:10.1108/09685220610655861

Imenda, S. (2014). Is there a conceptual difference between theoretical and conceptual frameworks? *Journal of Social Sciences*, *38*(2), 185–195. Retrieved from http://www.krepublishers.com/journalofsocialsciences.html

Ingham-Broomfield, R. (2014). A nurses' guide to quantitative research. *Australian Journal of Advanced Nursing*, *32*(2), 32–38. Retrieved from http://www.ajan.com.au

Irwin, S. (2013). Qualitative secondary data analysis: Ethics, epistemology and context. *Progress in Development Studies*, *13*, 295–306. doi:10.1177/1464993413490479

Ismail, S., Sitnikova, E., & Slay, J. (2014). Using integrated system theory approach to assess security for SCADA systems cyber security for critical infrastructures: A pilot study. *Institute of Electrical and Electronics Engineers*, 1000–1006. doi:10.1109/fskd.2014.6980976

Jacques, L. B. (2011). Electronic health records and respect for patient privacy: A prescription for compatibility. *Vanderbilt Journal of Entertainment and Technology Law*, *13*, 441–462. Retrieved from http://www.jetlaw.org/

Järveläinen, J. (2012). Information security and business continuity management in interorganizational IT relationships. *Information Management & Computer Security*, *20*, 332–349. doi:10.1108/09685221211286511

Jenkins, A., Anandarajan, M., & D'Ovidio, R. (2014). All that glitters is not gold: The role of impression management in data breach notification. *Western Journal of Communication*, *78*, 337–357. doi:10.1080/10570314.2013.866686

Jenkins, M. K. (2013). The dirty dozen healthcare IT issues. *AAOS Now*, *7*(11), 35–36. Retrieved from http://www.aaos.org

Jing, A., Brockett, P. L., Golden, L. L., & Guillén, M. (2013). A robust unsupervised method for fraud rate estimation. *Journal of Risk and Insurance*, *80*, 121–143. doi:10.1111/j.1539-6975.2012.01467.x

Johnson, B. (2014). Comply with regulations or risk paying hefty fines: Ten tips for choosing call recording to help ensure compliance. *The Journal of Medical Practice Management: MPM*, *29*, 290–300. Retrieved from http://www.mpmnetwork.com

Kamal, I. S. M., Mahmud, Z., Sulong, S., & Azid, N. N. N. (2014). Examining potential risk factors to acute pancreatitis disease: A comparison of loglinear models in a Malaysian case study. *Journal of Medical Sciences*, *14*, 153–161. doi:10.3923/jms.2014.153.161

Kamati, S. K. K., Cassim, N., & Karodia, A. M. (2014). An evaluation of the factors Influencing the performance of registered nurses at the national referral hospital in Namibia. *Australian Journal of Business and Management Research*, *4*(2), 47–62. Retrieved from http://www.ajbmr.com

Kamoun, F., & Nicho, M. (2014). Human and organizational factors of healthcare data breaches: The Swiss cheese model of data breach causation and prevention. *International Journal of Healthcare Information Systems and Informatics*, *9*(1), 42–60. doi:10.4018/ijhisi.2014010103

Kandola, D., Banner, D., O'Keefe-McCarthy, S., & Jassal, D. (2014). Sampling methods in cardiovascular nursing research: An overview. *Canadian Journal of Cardiovascular Nursing*, *24*(3), 15–18. Retrieved from https://www.cccn.ca

Kerr, P., DeAngelis, D., & Brown, T. G. A. (2014). Five questions to ask before a data breach occurs. *Journal of Health Care Compliance*, *16*(6), 27–71. Retrieved from http://www.aspenpublishers.com

Ketsman, O. (2012). Expectations in the foreign language classrooms: A case study. *The Qualitative Report*, *17*, 1–21. Retrieved from http://tqr.nova.edu/

Khan, S. N. (2014). Qualitative research method: Phenomenology. *Asian Social Science*, *10*(21), 298–310. doi:10.5539/ass.v10n21p298

Khey, D. N., & Sainato, V. A. (2013). Examining the correlates and spatial distribution of organizational data breaches in the United States. *Security Journal*, *26*, 367–382. doi:10.1057/sj.2013.24

Kieke, R. L. (2014). Recent privacy breach settlements illustrate the importance of proactively pursuing compliance. *Journal of Health Care Compliance*, *16*(4), 41–61. doi:10.2753/mis0742-1222300202

Kruger, C. J., & Mama, M. N. (2012). Incorporating business strategy formulation with identity management strategy formulation. *Information Management & Computer Security*, *20*, 152–169. doi:10.1108/09685221211247271

Kwan, B. S. C., Chan, H., & Lam, C. (2012). Evaluating prior scholarship in literature reviews of research articles: A comparative study of practices in two research

paradigms. *English for Specific Purposes*, *31*, 188–201. doi:10.1016/j.esp.2012.02.003

Kwon, J., & Johnson, M. E. (2013). Health-care security strategies for data protection and regulatory compliance. *Journal of Management Information Systems*, *30*, 41–66. doi:10.2753/MIS0742-1222300202

Kwon, J., & Johnson, M. E. (2014). Proactive versus reactive security investments in the healthcare sector. *MIS Quarterly*, *38*, 451–471. Retrieved from http://www.misq.org/

Lakshmi, S., & Mohideen, M. A. (2013). Issues in reliability and validity of research. *International Journal of Management Research and Reviews*, *3*, 2752–2758. Retrieved from http://ijmrr.com/

Lalor, J. G., Casey, D., Elliott, N., Coyne, I., Comiskey, C., Higgins, A., … Begley, C. (2013). Using case study within a sequential explanatory design to evaluate the impact of specialist and advanced practice roles on clinical outcomes: the SCAPE study. *BMC Medical Research Methodology*, *13*(55), 1–10. doi:10.1186/1471-2288-13-55

Langlois, L., Lapointe, C., Valois, P., & de Leeuw, A. (2014). Development and validity of the ehical leadership questionnaire. *Journal of Educational Administration*, *52*, 310–331. doi:10.1108/jea-10-2012-0110

Lawley, J. S. (2012). HIPAA, HITECH and the practicing counselor: Electronic records and practice guidelines. *The Professional Counselor*, *2*, 193–200. doi:10.15241/jsl.2.3.192

Layton, R., & Watters, P. A. (2014). A methodology for estimating the tangible cost of data breaches. *Journal of Information Security and Applications*, *19*(6), 321–330. doi:10.1016/j.jisa.2014.10.012

Lee, P. (2012). ePRO industry growth. *Applied Clinical Trials*, *21*(11), 6–7. Retrieved from http://www.appliedclinicaltrialsonline.com/

Lin, P.-Y., & Lin, Y.-C. (2014). Examining student factors in sources of setting accommodation DIF. *Educational and Psychological Measurement*, *74*, 759–794. doi:10.1177/0013164413514053

Liu, V., Musen, M., & Chou, T. (2015). Data breaches of protected health information in the United States. *JAMA*, *313*, 1471–1473. doi:10.1001/jama.2015.2252

Liu, Y., & De, A. (2015). Multiple imputation by fully conditional specification for dealing with missing data in a large epidemiologic study. *International Journal of Statistics in Medical Research*, *4*, 287–295. doi:10.6000/1929-6029.2015.04.03.7

Long, H. (2014). An empirical review of research methodologies and methods in creativity studies (2003–2012). *Creativity Research Journal*, *26*, 427–438. doi:10.1080/10400419.2014.961781

Loy, S. L., Brown, S., & Tabibzadeh, K. (2014). South Carolina Department of Revenue: Mother of government dysfunction. *Journal of the International Academy for Case Studies*, *20*(1), 83–93. Retrieved from http://www.academyforcasestudies.org

Lustgarten, S. D. (2015). Emerging ethical threats to client privacy in cloud communication and data storage. *Professional Psychology: Research and Practice*, *46*(3), 154–160. doi:10.1037/pro0000018

Marais, H. (2012). A multi-methodological framework for the design and evaluation of complex research projects and reports in business and management studies. *Electronic Journal of Business Research Methods*, *10*, 64–76. Retrieved from http://www.ejbrm.com

Markette, N. J. (2012). Prescriptions for high school administrative teams. *Team Performance Management*, *18*, 277–294. doi:10.1108/13527591211251113

Masic, I. (2012). Ethical aspects and dilemmas of preparing, writing and publishing of the scientific papers in the biomedical journals. *Acta Informatica Medica*, *20*, 141–148. doi:10.5455/aim.2012.20.141-148.

Masue, O. S., Swai, I. L., & Anasel, M. G. (2013). The qualitative-quantitative disparities in social science research: What does qualitative comparative analysis (qca) brings in to bridge the gap. *Asian Social Science*, *9*(10), 211–221. doi:10.5539/ass.v9n10p211

McDavid, J., & West, S. (2014). Corrective actions for HIPAA compliance in 2014: Practices focus on EHR system and record retention issues. *The Journal of Medical Practice Management: MPM*, *30*, 7–8. Retrieved from http://www.mpmnetwork.com

McNeal, M. (2014). Hacking health care. *Marketing Health Services*, *34*(3), 16–21. Retrieved from https://www.ama.org

Mettke-Hofmann, C., Hamel, P. B., Hofmann, G., Zenzal, T. J., Pellegrini, A., Malpass, J., … Greenberg, R. (2015). Competition and habitat quality influence age and sex distribution in wintering rusty blackbirds: e0123775. *PLoS One*, *10*(5), 1–17. doi:10.1371/journal.pone.0123775

Mobargha, N., Ludwig, C., Ladd, A. L., & Hagert, E. (2014). Ultrastructure and innervation of thumb carpometacarpal ligaments in surgical patients with osteoarthritis. *Clinical Orthopaedics and Related Research*, *472*, 1146–1154. doi:10.1007/s11999-013-3083-7

Mofidi, M., & Shoushtari, Z. G. (2012). A comparative study of the complaint strategies among Iranian EFL and ESL students: The study of the effect of length of residence and the amount of contact. *English Language Teaching*, *5*(11), 118–124. doi:10.5539/elt.v5n11p118

Morgan, D. L. (2015). From themes to hypotheses: Following up with quantitative methods. *Qualitative Health Research*, *25*, 789–793. doi:10.1177/1049732315580110

Mrayyan, M. T. (2006). Invest in yourself: The internet: Uses in administrative research and practice. *Nursing Forum*, *41*, 41–45. doi:10.1111/j.1744-6198.2006.00036.x

Nelson, J. M. (2012). Taking community seriously: A theory and method for a community-oriented psychology of religion. *Pastoral Psychology*, *61*, 851–863. doi:10.1007/s11089-012-0454-z

Newman, I., & Covrig, D. M. (2013). Building consistency between title, problem statement, purpose, & research questions to improve the quality of research plans

and reports. *New Horizons in Adult Education & Human Resource Development*, *25*(1), 70–79. doi:10.1002/nha.20009

Nodoushan, M. A. S. (2014). Speech acts or language micro- and macro-games? *International Journal of Language Studies*, *8*(4), 1–28. doi:10.13140/2.1.3699.2648

Öğüş, E., & Yazıcı, A. C. (2011). Comparison of log-linear analysis and correspondence analysis in two-way contingency tables: A medical application. *Balkan Medical Journal*, *28*, 143–147. doi:10.5174/tutfd.2009.03375.1

Ojedokun, U. A. (2012). Trafficking in Nigerian cultural antiquities: A criminological perspective. *African Journal of Criminology and Justice Studies : AJCJS*, *6*(1), 163–176. Retrieved from www.umes.edu

Okoli, C. N., Onyeagu, S. I., & Osuji, G. A. (2015). A generalized method for estimating parameters and model of best fit in log-linear models. *European Journal of Statistics and Probability*, *3*(1), 1–12. Retrieved from http://www.eajournals.org/journals/european-journal-of-statistics-and-probability-ejsp

Olayemi, O. J. (2014). A socio-technological analysis of cybercrime and cyber security in Nigeria. *International Journal of Sociology and Anthropology*, *6*(3), 116–125. doi:10.5897/ijsa2013.0510

Olmuş, H., & Erbaş, S. (2012). Analysis of traffic accidents caused by drivers by using log-linear models. *PROMET-Traffic&Transportation*, *24*, 495–504. doi:10.1002/nha.20009

Onder, M., Onder, S., & Mutlu, A. (2012). Determination of noise induced hearing loss in mining: an application of hierarchical loglinear modelling. *Environmental Monitoring and Assessment*, *184*, 2443–2451. doi:10.1007/s10661-011-2129-0

Ozair, F. F., Jamshed, N., Sharma, A., & Aggarwal, P. (2015). Ethical issues in electronic health records: A general overview. *Perspectives in Clinical Research*, *6*, 73–76. doi:10.4103/2229-3485.153997

Patrician, P. A., Loan, L., McCarthy, M., Brosch, L. R., & Davey, K. S. (2010). Towards evidence-based management: Creating an informative database of nursing-sensitive indicators. *Journal of Nursing Scholarship*, *42*, 358–366. doi:10.1111/j.1547-5069.2010.01364.x

Paull, M., Boudville, I., & Sitlington, H. (2013). Using sensemaking as a diagnostic tool in the analysis of qualitative data. *The Qualitative Report*, *18*, 1–12. Retrieved from http://tqr.nova.edu/

Pavlović, M., Milković-Kraus, S., Jovanović, V., & Hercigonja-Szekeres, M. (2012). Ageing, arterial blood pressure, body mass index, and diet. *Arh Hig Rada Toksikol*, *63*(Supplement 1), 3–9. doi:10.2478/10004-1254-63-2012-2164

Perakslis, E. D. (2014). Cybersecurity in health care. *The New England Journal of Medicine*, *371*, 395–397. doi:10.1056/nejmp1404358

Pérez-Rodríguez, A., de la Hera, I., Bensch, S., & Pérez-Tris, J. (2015). Evolution of seasonal transmission patterns in avian blood-borne parasites. *International Journal for Parasitology*, *45*, 605–611. doi:10.1016/j.ijpara.2015.03.008

Pesonen, H.-M., Remes, A. M., & Isola, A. (2011). Ethical aspects of researching subjective experiences in early-stage dementia. *Nursing Ethics*, *18*, 651–661. doi:10.1177/0969733011408046

Peterson, N. E., Moss, K. O., Milbrath, G. R., von Gaudecker, J. R., Park, E., & Chung, M. (2015). Qualitative analysis of student perceptions of bachelor of science-to-doctor of philosophy in nursing programs. *Journal of Nursing Education*, *54*, 542–549. doi:10.3928/01484834-20150916-01

Petitjean, F., Allison, L., & Webb, G. I. (2014). A statistically efficient and scalable method for log-linear analysis of high-dimensional data. In *IEEE International Conference on Data Mining* (pp. 480–489). Shenzhen: IEE. doi:10.1109/ICDM.2014.23

Pevnick, J. M., Claver, M., Dobalian, A., Asch, S. M., Stutman, H. R., Tomines, A., & Fu, P. (2012). Provider stakeholders' perceived benefit from a nascent health information exchange: A qualitative analysis. *Journal of Medical Systems*, *36*, 601–613. doi:10.1007/s10916-010-9524-x

Pfefferbaum, B., Weems, C. F., Scott, B. G., Nitiéma, P., Noffsinger, M. A., Pfefferbaum, R. L., … Chakraburtty, A. (2013). Research methods in child disaster studies: A review of studies generated by the September 11, 2001, terrorist attacks; the 2004 Indian Ocean Tunami; and Hurricane Katrina. *Child & Youth Care Forum*, *42*, 285–337. doi:10.1007/s10566-013-9211-4

Pickering, C., & Byrne, J. (2014). The benefits of publishing systematic quantitative literature reviews for PhD candidates and other early-career researchers. *Higher*

Education Research & Development, *33*, 534–548. doi:10.1080/07294360.2013.841651

Plunkett, L. (2013). That which makes your life easier can also cause chaos. *New York State Dental Journal*, *79*(2), 7–12. Retrieved from https://nysdental.org

Pomerantseva, V., & Ilicheva, O. (2011). Clinical data collection, cleaning and verification in anticipation of database lock. *Pharmaceutical Medicine*, *25*, 223–233. doi:10.1007/bf03256864

Price, & Murnan, J. (2004). Research limitations and the necessity of reporting them. *American Journal of Health Education*, *35*, 66–67. doi:10.1080/19325037.2004.10603611

Rahimifar, M., & Salim, S. (2012). Structuring persistent chat conversations: experimental results of the chatsistance tool. *Knowledge & Information Systems*, *33*, 685–705. doi:10.1007/s10115-012-0536-3

Rahman, R., & Gul, H. (2014). Conversation analysis: Speech acts in Ibsen's a doll's house. *The Journal of Humanities and Social Sciences*, *22*(1), 67–82. Retrieved from www.ijhssnet.com/

Rajakumar, M. P., & Shanthi, V. (2014). Security breach in trading system-countermeasure using Iptraceback. *American Journal of Applied Sciences*, *11*, 492–498. doi:10.3844/ajassp.2014.492.498

Redman-Maclaren, M., Mills, J., & Tommbe, R. (2014). Interpretive focus groups: a participatory method for interpreting and extending secondary analysis of qualitative data. *Global Health Action*, *7*. doi:10.3402/gha.v7.25214

Rey, J., & Douglass, K. (2012). Keys to securing data as a practitioner. *The Journal of Medical Practice Management: MPM*, *27*(4), 203–205. Retrieved from http://www.mpmnetwork.com

Ringim, K. J., Razalli, M. R., & Hasnan, N. (2012). A framework of business process re-engineering factors and organizational performance of Nigerian banks. *Asian Social Science*, *8*(4), 203–216. doi:10.5539/ass.v8n4p203

Rinke, E. M., Wessler, H., Löb, C., & Weinmann, C. (2013). Deliberative qualities of generic news frames: Assessing the democratic value of strategic game and contestation framing in election campaign coverage. *Political Communication*, *30*, 474–494. doi:10.1080/10584609.2012.737432

Roberts, J. (2014). The necessity of information security in the vulnerable pharmaceutical industry. *Journal of Information Security*, *5*, 147–153. doi:10.4236/jis.2014.54014

Roda, C., Nicolis, I., Momas, I., & Guihenneuc, C. (2014). New insights into handling missing values in environmental epidemioloegical studies: e104254. *PLoS One*, *9*(9), 1–8. doi:10.1371/journal.pone.0104254

Rodrigues, J. J. P. C., de la Torre, I., Fernández, G., & López-Coronado, M. (2013). Analysis of the security and privacy requirements of cloud-based electronic health records systems. *Journal of Medical Internet Research*, *15*, 418–426. doi:10.2196/jmir.2494

Rogers, W., & Lange, M. M. (2013). Rethinking the vulnerability of minority populations in research. *American Journal of Public Health*, *103*, 2141–2146. doi:10.2105/ajph.2012.301200

Romanosky, S., Acquisti, A., & Telang, R. (2011). Do data breach disclosure laws reduce identity theft? *Journal of Policy Analysis & Management*, *30*, 256–286. doi:10.1002/pam.20567

Romanosky, S., Hoffman, D., & Acquisti, A. (2014). Empirical analysis of data breach litigation. *Journal of Empirical Legal Studies*, *11*(1), 74–104. doi:10.1111/jels.12035

Rothstein, M. A. (2013). HIPAA privacy rule 2.0. *Journal of Law, Medicine & Ethics*, *41*(2), 525–528. doi:10.1111/jlme.12060

Roy, D. J. (2014). Unexamined assumptions in palliative care. *Journal of Palliative Care*, *30*(4), 251–254. Retrieved from http://www.criugm.qc.ca/journalofpalliativecare/

Sacopulos, M. J., & Segal, J. (2014). Business associates gone bad: Five tales of woe and ways to prevent them from happening to you. *The Journal of Medical Practice Management: MPM*, *30*, 84–88. Retrieved from http://www.mpmnetwork.com

Salter, D. W. (2003). Log-linear techniques for the analysis of categorical data: A demonstration with the myers-briggs type indicator. *Measurement and Evaluation in Counseling and Development*, *36*, 106–121. Retrieved from http://mec.sagepub.com

Sampson, J. P., Hou, P.-C., Kronholz, J. F., Dozier, V. C., McClain, M.-C., Buzzetta, M., … Kennelly, E. L. (2014). A content analysis of career development theory, research, and practice-2013. *The Career Development Quarterly*, *62*, 290–326. doi:10.1002/j.2161-0045.2014.00085.x

Sauers, E. L., McLeod, T. C. V., & Bay, R. C. (2012). Practice-based research networks, Part I: Clinical laboratories to generate and translate research findings into effective patient care. *Journal of Athletic Training*, *47*, 549–556. doi:10.4085/1062-6050-47.5.11.

Sauls, J., & Gudigantala, N. (2013). Preparing information systems (IS) graduates to meet the challenges of global IT security: Some suggestions. *Journal of Information Systems Education*, *24*, 71–73. Retrieved from http://jise.org/

Schulke, D. F. (2013). The regulatory arms race: Mobile-health applications and agency posturing. *Boston University Law Review*, *93*, 1699–1752. Retrieved from http://www.bu.edu/bulawreview/

Schuster, C. P., Anderson, B., & Brodowsky, G. (2014). Secondary data: Collection and analysis - Classroom activities for learning. *Journal of the Academy of Business Education*, *15*(Spring), 97–118. Retrieved from http://www.abeweb.org/jbe.html

Selamat, M. H., & Babatunde, D. A. (2014). Mediating effect of information security culture on the relationship between information security activities and organizational performance in the Nigerian banking setting. *International Journal of Business and Management*, *9*(7), 33–38. doi:10.5539/ijbm.v9n7p33

Sen, R., & Borle, S. (2015). Estimating the contextual risk of data breach: An empirical approach. *Journal of Management Information Systems*, *32*(2), 314–341. doi:10.1080/07421222.2015.1063315

Sharma, S., & Sugumaran, V. (2011). A framework for enhancing systems security. *Journal of Information Privacy & Security*, *7*(4), 3–22. doi:10.1080/15536548.2011.10855921

Shin, M. S., Jeon, H. S., Ju, Y. W., Lee, B. J., & Jeong, S.-P. (2015). Constructing RBAC based security model in u-healthcare service platform. *The Scientific World Journal*, *2015: 265132*. doi:10.1155/2015/937914

Shorten, A., & Moorley, C. (2014). Selecting the sample. *Evidence Based Nursing*, *17*, 32–33. doi:10.1136/eb-2014-101747

Siddiqui, N., & Fitzgerald, J. A. (2014). Elaborated integration of qualitative and quantitative perspectives in mixed methods research: A profound enquiry into the nursing practice environment. *International Journal of Multiple Research Approaches*, *8*, 137–147. doi:10.1080/18340806.2014.11082056

Sikorskii, A., & Noble, P. C. (2013). Statistical considerations in the psychometric validation of outcome measures. *Clinical Orthopaedics and Related Research*, *471*, 3489–3495. doi:10.1007/s11999-013-3028-1

Silverman, D. L. (2014). Developments in data security breach liability. *Business Lawyer*, *70*, 231–245. Retrieved from http://www.americanbar.org/publications/the_business_lawyer.html

Sinclair, J. P., Emlen, J., & Freeman, D. C. (2012). Biased sex ratios in plants: Theory and trends. *The Botanical Review*, *78*, 63–86. doi:10.1007/s12229-011-9065-0

Sindhuja, P. N. (2014). Impact of information security initiatives on supply chain performance. *Information Management & Computer Security*, *22*, 450–473. doi:10.1108/imcs-05-2013-0035

Sloane, D., & Morgan, S. P. (1996). An introduction to categorical data analysis. *Annual Review of Sociology*, *22*, 351–375. doi:10.1146/annurev.soc.22.1.351

Smyth, S. M. (2014). The greening of Canadian cyber laws: What environmental law can teach and cyber law can learn. *International Journal of Cyber Criminology*, *8*, 111–155. Retrieved from http://www.cybercrimejournal.com

Sousa, V. D., Driessnack, M., & Mendes, I. A. C. (2007). An overview of research designs relevant to nursing: Part 1: Quantitative research designs. *Revista Latino-Americana de Enfermagem*, *15*, 502–507. doi:10.1590/s0104-11692007000300022

Srivastava, H., & Kumar, S. A. (2015). Control framework for secure cloud computing. *Journal of Information Security*, *6*, 12–23. doi:10.4236/jis.2015.61002

Sterling, R. (2015). Defend your practice against HIPAA violations. *Contemporary Pediatrics*, *32*(4), 34–37. Retrieved from http://contemporarypediatrics.modernmedicine.com/

Strauss, L. J. (2014). Compliance and enforcement related to privacy, security, and breach notification rules. *Journal of Health Care Compliance*, *16*(6), 23–26. Retrieved from http://www.wklawbusiness.com

Suguna, R., Kujani, T., Suganya, N., & Krishnaveni, C. (2014). Hunting pernicious attacks in web applications with xprober. *American Journal of Applied Sciences*, *11*, 1164–1171. doi:10.3844/ajassp.2014.1164.1171

Sullivan, S. A., Wiles, N., Kounali, D., Lewis, G., Heron, J., Cannon, M., … Zammit, S. (2014). Longitudinal associations between adolescent psychotic experiences and depressive symptoms: e105758. *PLoS One*, *9*(8), 1–7. doi:10.1371/journal.pone.0105758

Tansey, R., White, M., Long, R. G., & Smith, M. (1996). A comparison of loglinear modeling and logistic regression in management research. *Journal of Management*, *22*, 339–358. Retrieved from http://jom.sagepub.com/

Taylor, R. G., & Robinson, S. L. (2015). An information system security breach at First Freedom Credit Union: What goes in must come out. *Journal of the International Academy for Case Studies*, *21*(1), 131–138. Retrieved from http://www.academyforcasestudies.org

Telang, R. (2015). Policy framework for data breaches. *IEEE Security & Privacy*, *13*(1), 77–79. doi:10.1109/msp.2015.12

Toledo, A. H., Flikkema, R., & Toledo-Pereyra, L. H. (2011). Developing the research hypothesis. *Journal of Investigative Surgery*, *24*, 191–194. doi:10.3109/08941939.2011.609449

Tomczak, M., Tomczak, E., Kleka, P., & Lew, R. (2014). Using power analysis to estimate appropriate sample size. *Trends in Sport Sciences*, *21*, 195–206. doi:10.1148/radiol.2272012051

Tomkinson, S. (2015). Doing fieldwork on state organizations in democratic settings: Ethical issues of research in refugee decision making. *Forum : Qualitative Social Research*, *16*(1), n/a. Retrieved from http://www.qualitative-research.net/index.php/fqs

Tu, M., Spoa-Harty, K., & Xiao, L. (2015). Data loss prevention and control: Inside activity incident monitoring, identification, and tracking in healthcare enterprise environments. *The Journal of Digital Forensics, Security and Law : JDFSL*, *10*(1), 27–44. Retrieved from http://www.jdfsl.org/

Turner, T. L., Balmer, D. F., & Coverdale, J. H. (2013). Methodologies and study designs relevant to medical education research. *International Review of Psychiatry*, *25*, 301–310. doi:10.3109/09540261.2013.790310

Unluer, S. (2012). Being an insider researcher while conducting case study research. *Qualitative Report*, *17*, 1–14. Retrieved from http://tqr.nova.edu/

Vaid, D. (2012). The caste-class association in India. *Asian Survey*, *52*, 395–422. doi:10.1525/as.2012.52.2.395

van der Meulen, N. (2013). DigiNotar: Dissecting the first Dutch digital disaster. *Journal of Strategic Security*, *6*(2), 46–58. doi:10.5038/1944-0472.6.2.4

van Middendorp, J. J., Patel, A. A., Schuetz, M., & Joaquim, A. F. (2013). The precision, accuracy and validity of detecting posterior ligamentous complex injuries of the thoracic and lumbar spine: a critical appraisal of the literature. *European Spine Journal*, *22*, 461–474. doi:10.1007/s00586-012-2602-7

Vockley, M. (2012). Safe and secure healthcare in the cyberworld. *Biomedical Instrumentation & Technology*, *46*, 164–173. doi:10.2345/0899-8205-46.3.164

Wall, D. S. (2013). Enemies within: Redefining the insider threat in organizational security policy. *Security Journal*, *26*, 107–124. doi:10.1057/sj.2012.1

Wan, Z., Vorobeychik, Y., Xia, W., Clayton, E. W., Kantarcioglu, M., Ganta, R., … Malin, B. A. (2015). A game theoretic framework for analyzing re-identification risk: e0120592. *PLoS One*, *10*(3), 1–24. doi:10.1371/journal.pone.0120592

Weisse, A. B. (2014). HIPAA: A flawed piece of legislation. *Baylor University Medical Center Proceedings*, *27*, 163–165. doi:10.1353/pbm.2013.0003

Welford, C., Murphy, K., & Casey, D. (2012). Demystifying nursing research terminology: Part 2. *Nurse Researcher*, *19*(2), 29–35. doi:10.7748/nr2012.01.19.2.29.c8906

Weller, D., Vedsted, P., Rubin, G., Walter, F. M., Emery, J., Scott, S., … Neal, R. D. (2012). The aarhus statement: Improving design and reporting of studies on early cancer diagnosis. *British Journal of Cancer*, *106*, 1262–1267. doi:10.1038/bjc.2012.68

Wester, K. L. (2011). Publishing ethical research: A step-by-step overview. *Journal of Counseling and Development: JCD*, *89*, 301–307. doi:10.1002/j.1556-6678.2011.tb00093.x

Whiteley, A. (2012). Supervisory conversations on rigour and interpretive research. *Qualitative Research Journal*, *12*, 251–271. doi:10.1108/14439881211248383

White, M., Tansey, R., & Smith, M. (1994). A causal modelling test of the relationship between chief executive officer experience and corporate strategy. *Journal of Occupational & Organizational Psychology*, *67*, 259–278. doi:10.1111/j.2044-8325.1994.tb00566.x

White, M., Tansey, R., Smith, M., & Barnett, T. (1993). Log-linear modeling in personnel research. *Personnel Psychology*, *46*, 667–686. doi:10.1111/j.1744-6570.1993.tb00890.x

Whiteside, M., Mills, J., & Mccalman, J. (2012). Using secondary data for grounded theory analysis. *Australian Social Work*, *65*, 504–516. doi:10.1080/0312407x.2011.645165

Wikina, S. B. (2014). What caused the breach? An examination of use of information technology and health data breaches. *Perspectives in Health Information Management*, *11*(Fall), 1–16. Retrieved from http://perspectives.ahima.org

Wilkes, J. J. (2014). The creation of HIPAA culture: prioritizing privacy paranoia over patient care. *Brigham Young University Law Review*, *2014*, 1213–1249. Retrieved from http://digitalcommons.law.byu.edu/lawreview/

Willey, L., & White, B. J. (2013). Do you take credit cards? Security and compliance for the credit card payment industry. *Journal of Information Systems Education*, *24*, 181–188. Retrieved from http://jise.org/

Williams, P. A. H., & Hossack, E. (2013). It will never happen to us: The likelihood and impact of privacy breaches on health data in Australia. *Studies in Health*

Technology and Informatics, *188*(1), 155–161. doi:10.3233/978-1-61499-266-0-155

Wirth, A. (2012). Enabling mHealth while assuring compliance: Reliable and secure information access in a mobile world. *Biomedical Instrumentation & Technology*, *46*, 91–96. doi:10.2345/0899-8205-46.s2.91

Wright, B., & Ogbuehi, A. O. (2014). Surveying adolescents: The impact of data collection methodology on response quality. *Electronic Journal of Business Research Methods*, *12*, 41–53. Retrieved from http://www.ejbrm.com

Wright, M. A., & Drozdenko, R. G. (2013). Implications of student perceptions regarding the disclosure of sensitive information. *Journal of Leadership, Accountability and Ethics*, *10*(3), 79–97. Retrieved from http://whttp://www.na-businesspress.com

Yoshikawa, H., Weisner, T. S., Kalil, A., & Way, N. (2013). Mixing qualitative and quantitative research in developmental science: Uses and methodological choices. *Qualitative Psychology*, *1*(S), 3–18. doi:10.1037/2326-3598.1.S.3

Young, R., & Johnson, D. (2013). Methods for handling missing secondary respondent data. *Journal of Marriage and Family*, *75*, 221–234. doi:10.1111/j.1741-3737.2012.01021.x

Zelle, A. R., & Whitehead, S. M. (2014). Cyber liability: It's just a click away. *Journal of Insurance Regulation*, *33*(6), 145–168. Retrieved from http://www.naic.org/

Zheng, G., Lan, X., Li, M., Ling, K., Lin, H., Chen, L., … Fang, Q. (2015). Effectiveness of Tai Chi on physical and psychological health of college students: Results of a

randomized controlled trial: e0132605. *PLoS One*, *10*(7), 1–14. doi:10.1371/journal.pone.0132605

Zhu, B., Walter, S. D., Rosenbaum, P. L., Russell, D. J., & Raina, P. (2006). Structural equation and log-linear modeling: a comparison of methods in the analysis of a study on caregivers' health. *BMC Medical Research Methodology*, *6*, 49. doi:10.1186/1471-2288-6-49

Zohrabi, M. (2013). Mixed method research: Instruments, validity, reliability and reporting findings. *Theory and Practice in Language Studies*, *3*, 254–262. doi:10.4304/tpls.3.2.254-262