2018

Risk in Privacy Breach Determination: The Application of Prospect Theory to Healthcare Privacy Officers

Amanda Walden
University of Central Florida

RISK IN PRIVACY BREACH DETERMINATION: THE APPLICATION OF PROSPECT THEORY TO HEALTHCARE PRIVACY OFFICERS

by

AMANDA WALDEN
B.S. University of Central Florida, 2007
M.S. University of Central Florida, 2009

A dissertation submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
in the Department of Public Affairs
in the College of Community Innovation and Education
at the University of Central Florida
Orlando, Florida

Fall Term
2018

Major Professor: Kendall Cortelyou-Ward

ABSTRACT

A significant concern in healthcare is that of patient privacy and how organizations protect against unauthorized access to protected health information. The federal government has responded by instituting policies and guidelines on requirements for protection. However, the policy language leaves areas open to interpretation by those following the guidelines. Reporting to the Office for Civil Rights and/or the patient can open an organization to risk of financial and possible criminal penalties. There is a risk of harm to their reputation which could impact patient visits and market share. Therefore, Privacy Officers might view risk in different ways and therefore handle breach reporting differently. Privacy Officers are responsible for determining an individual organization's breach reportability status. Their processes may vary dependent on their knowledge of the policy, the status of previous reported breaches, and their framing of an incident. This research aims to explore the following factors: (1) personal and organizational knowledge, (2) prior breach status, (3) and scenario framing, to explore if Prospect Theory is applicable to the choices a Privacy Officer makes regarding breach determination. The study uses primary data collection through a survey that includes loss and gain scenarios in accordance with Prospect Theory. Individuals listed as Privacy Officers within the American Health Information Management Association (AHIMA) were the target audience for the survey. Univariate, Bivariate, Multivariate, and Post Regression techniques were used to analyze the data collected. The findings of the study supported the theoretical framework and provided industry and public affairs implications. These findings show that there is a gap where Privacy Officers have to make their own decisions and there is a difference in the types of decisions they are

making on a day to day basis. Future guidance and policies need to address these gaps and can use the insight provided by this study.

Keywords: Healthcare, Privacy, Breach, Privacy Officer, Prospect Theory

This dissertation is dedicated to my husband Patrick. Your unending love and support is the reason I was able to complete this program. This accomplishment is thanks to you.

To my daughter Emma, while your arrival during this process was an additional step, it was the best I have ever taken. I hope this can inspire you one day, that you can accomplish anything you aspire to.

To my mother, Kathy, your uplifting spirit was the light in the dark. Without you I would not have achieved this.

To my father, Jeff, you have always strived for greatness. It was with this example that I have pursued my education and career.

To my sister, Kelly, while you are miles away your support crossed the distance with ease. Thank you for being my sounding board and shoulder to lean on.

ACKNOWLEDGMENTS

There are many people who assisted in this journey. First, thank you to my committee chair, Dr. Kendall Cortelyou-Ward. Your willingness to serve and help throughout this process was critical to the success of the study. You have provided a shining example of what someone in our field is capable of and it has served as something for me to strive towards. My committee has provided a significant amount of time and dedication to this study as well. Dr. Alice Noblin, you have been a constant in my life from the beginning of my career at the University of Central Florida almost 15 years ago. It was your inspiring take on the Health Information Management field during freshman orientation that set me on this path, and your endless encouragement and support throughout this time has meant the world to me. I can honestly say I would not be where I am without you.

Dr. Meghan Hufstader Gabriel, while our career together has not been long, you have provided a significant amount of time and support for this process. Your knowledge was key to the success of this paper, thank you for your dedication. Dr. Claire Knox, your insight to Public Administration and Public Affairs brought a new set of eyes to this topic which allowed me to look at it from different angles. I am thankful for the knowledge and mindset you brought to this process. I also need to express my gratitude to Kelly McLendon who served as the subject matter expert. His willingness to assist was instrumental in the success of this study.

Thank you to the faculty and staff of the Public Affairs program. You all have been great teachers and mentors, willing to hold our hands and help see us through. Thank you as well to the faculty and staff of the Health Management and Informatics Department. Without your support this would not be possible.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS (or) ABBREVIATIONS

AHIMA- American Health Information Management Association

ARRA – American Recovery and Reinvestment Act

CE – Covered Entity

DHHS- Department of Health and Human Services

HIPAA – Health Insurance Portability and Accountability Act

HITECH- Health Information Technology for Economic and Clinical Health

NIH – National Institute of Health

OCR- Office for Civil Rights

PHI- Protected Health Information

RHIA- Registered Health Information Administrator

CHAPTER ONE: INTRODUCTION

The following chapter outlines the state of patient privacy including current federal policy, details the significance, discusses the theoretical framework, and describes the methodological approach of the study.

State of Patient Privacy

The Health Insurance Portability and Accountability Act (HIPAA) passed on August 21, 1996, was enacted to, among other things, help protect the privacy and security of a patient's protected health information (PHI) (LaTour & Eichenwald-Maki, 2006). This legislation established patient rights to their healthcare information as well as restrictions on breaches (unauthorized disclosures of patient information). However, it lacked enforcement capabilities by the federal government, which negated its effects (Collins, 2007).

Under the American Recovery and Reinvestment Act (ARRA), a portion of the Health Information Technology for Economic and Clinical Health (HITECH) Act strengthened HIPAA laws including enforcement, penalties, and breach notification (LaTour & Eichenwald-Maki, 2006). The breach language was vague, so in 2013 the Omnibus Final Rule passed to clarify the ambiguities (Wilder, Bennett, Bianchi, & Peters, 2013). The Final Rule updated some key terminology; however, it did not provide strict guidance to identify reportable breaches. This has left gaps in the legislation where individuals and organizations are making decisions about patient privacy concerns.

Significance of the Study

The legislation requires that facilities designate privacy officials as the individuals in a healthcare organization responsible for identifying, determining, and reporting breaches of

patient privacy to the oversight body, the Office for Civil Rights (Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules, 2013; Liginlal, Sim, Khansa & Fearn, 2012). Many facilities have termed this position as a Privacy Officer. A problem not previously identified is whether the Privacy Officers of organizations are weighing the implications of reporting and if that knowledge is affecting their choices to report breaches that do occur to the Office for Civil Rights, the oversight body. This problem is identified as a public affairs issue as it impacts governance policy, public practices, and individual patient concerns.

If a privacy breach occurs, Privacy Officers make essential choices, based on organizational knowledge, which can affect the well-being of patients. Federal policy tends to be intentionally vague for operational purposes and moves slowly in terms of updating for current trends (Salamon, 2002). In 2016, the Government Accountability Office recommended that the Department of Health and Human Services increase their oversight of security and privacy guidance provided to healthcare facilities covered by HIPAA legislation (2016). Their investigation found that, due to the increased use of electronic health records, there is more vulnerability of patient information to cyber-based threats (GAO, 2016).

While there are guidelines, in the case of HIPAA and breach notifications, the organization and its Privacy Officer(s) determine whether to report a breach. Therefore, there is a need to understand if these individuals make the best choice for patients and not just the right choice for their organization. There are high costs associated with maintaining patient privacy as well as high costs when patient privacy is breached which may be taken into account when deciding whether to report a breach (Coate & MacDonald, 2002; Fleming, Culler, McCorkel, Becker, & Ballard, 2011; Adler-Milstein, Green, & Bates, 2013; McMillan, 2015; Khansa et.al,

2012; Ponemon, 2012; 2013; 2014; 2015; 2016; Campbell, Gordon, Loeb & Zhou, 2003; Khansa & Liginlal, 2009; Andoh-Baido & Bryson, 2006). Breaches to privacy of healthcare information can be detrimental to patients in many ways, including the emotional upheaval of the knowledge that others may have access to their personal medical information, the potential financial and identity theft, and actual harm from unnecessary or unobtainable treatment if an unauthorized user expends their available services or receives treatment, which ends up on the patient's record as the patient's history (Korolov, 2015; Amori, 2008).

Theoretical Framework

This study aims to understand how Privacy Officers are making choices about breach determination. Prospect Theory is the framework used to guide the study. Prospect theory is robust and has many implications for management and healthcare. The theory evolved over 300 years from the concept of utility to Risk Theory to Prospect Theory (Tversky & Kahneman, 1992). Throughout the years the research has built upon the exiting foundation, keeping the original constructs and adding new ones with each iteration to include Utility, Diminishing Marginal Utility, Risk Behavior, Reference Points, Value Functions, Weighting, Framing, and Loss Aversion (Arrow, 1971; Briggs 2015; Bernoulli, 1738; Kahneman & Tversky, 1979; Tversky & Kahneman, 1991). For this study, Prospect Theory is used to examine individual choices based on prior knowledge (reference points), framing effects (loss or gain), and decision weights (Kahneman & Tversky, 1979).

Prospect theory finds that an individual will take a risk in proportion to their utility from the outcome, their satisfaction level with the chance of gain, rather than taking into account the proportion that the gain will occur (Bernoulli, 1738). However, utility does not increase at a

consistent rate and the more one has of something, the increase in utility diminishes (Marshall, 1890; Holmes et al., 2011). Individuals fall into one of three categories (i.e., risk averse, risk neutral, and risk seeking), which affects behavior and when evaluating gains, a person is risk averse and when evaluating losses, a person is risk seeking (Pratt, 1964; Arrow, 1971; Kahneman & Tversky, 1979). Actual probabilities are overweighted or underweighted when deciding whether to take a risk. Framing indicates that the outcome of risk will determine willingness to take the risk, if the outcome is a gain, the likelihood of an individual taking the risk falls on a convex or concave curve dependent on the outcome of the risk (Kahneman & Tversky, 1979). Loss aversion simulates that a person will feel a loss harder than a gain and that hurt from a loss plateaus (Tversky & Kahneman, 1991).

Prospect Theory in healthcare research is still relatively new. The theory has been used for individual behavior for quite some time; however, its implications to management/healthcare analysis is wide open. This theoretical framework helps to explain a Privacy Officer's view of the risk of potential privacy breaches. A conceptual map was created using the theory's constructs and this was used to formulate a survey for analysis.

Methodological Approach

The research questions and hypotheses for this study are as follows:

RQ1: Does the Privacy Officers' reference point based on knowledge levels affect their choice to report a breach of patient information?

H1: Higher percentage of years employed in the healthcare field is positively associated with reporting future indefinable breaches of healthcare information in a general scenario.

H2: Higher percentage of years employed in the healthcare field is positively associated with reporting future indefinable breaches of healthcare information in a gain scenario.

H3: Higher percentage of years employed in the healthcare field is positively associated with reporting future indefinable breaches of healthcare information in a loss scenario.

H4: Lower level of self-reported knowledge in healthcare privacy is negatively associated with reporting future indefinable breaches of healthcare information in a general scenario.

H5: Lower level of self-reported knowledge in healthcare privacy is negatively associated with reporting future indefinable breaches of healthcare information in a gain scenario.

H6: Lower level of self-reported knowledge in healthcare privacy is negatively associated with reporting future indefinable breaches of healthcare information in a loss scenario.

H7: Higher levels of education are positively associated with reporting future indefinable breaches of healthcare information in a general scenario.

H8: Higher levels of education are positively associated with reporting future indefinable breaches of healthcare information in a gain scenario.

H9: Higher levels of education are positively associated with reporting future indefinable breaches of healthcare information in a loss scenario.

H10: Attainment of a Certified Healthcare Privacy and Security credential is positively associated with reporting future indefinable breaches of healthcare information in a general scenario.

H11: Attainment of a Certified Healthcare Privacy and Security credential is positively associated with reporting future indefinable breaches of healthcare information in a gain scenario.

H12: Attainment of a Certified Healthcare Privacy and Security credential is positively associated with reporting future indefinable breaches of healthcare information in a loss scenario.

H13: Attainment of a Registered Health Information Administrator or Technician credential is positively associated with reporting future indefinable breaches of healthcare information in a general scenario.

H14: Attainment of a Registered Health Information Administrator or Technician credential is positively associated with reporting future indefinable breaches of healthcare information in a gain scenario.

H15: Attainment of a Registered Health Information Administrator or Technician credential is positively associated with reporting future indefinable breaches of healthcare information in a loss scenario.

RQ2: Does the Privacy Officers' reference points based on past reporting affect their choice to report a breach of patient information?

H16: Prior reporting of a breach of healthcare information to the Office for Civil Rights is positively associated with reporting future indefinable breaches of healthcare information in a general scenario.

H17: Prior reporting of a breach of healthcare information to the Office for Civil Rights is positively associated with reporting future indefinable breaches of healthcare information in a gain scenario.

H18: Prior reporting of a breach of healthcare information to the Office for Civil Rights is positively associated with reporting future indefinable breaches of healthcare information in a loss scenario.

RQ3: Does the framing of a scenario affect Privacy Officers' choice to report a breach of information?

H19: A breach of healthcare information scenario framed as a gain is positively associated with privacy officers classifying the breach as reportable to the Office for Civil Rights.

H20: A breach of healthcare information scenario framed as a loss is negatively associated with privacy officers classifying the breach as reportable to the Office for Civil Rights.

The population targeted for this study is American Health Information Management Association (AHIMA) affiliated Privacy Officers. This specific population is the focus due to HIPAA regulations that all healthcare covered entities designate a Privacy Officer to be responsible for facility requirements. Privacy Officers are likely to be AHIMA members due to the nature of the regulations, ensuring access, privacy, and security of patient records. The AHIMA mission states "Transforming healthcare by leading HIM, Informatics, and Information Governance" (AHIMA, 2018, para. 1). Survey questionnaires, created with Prospect Theory, included demographic and personal information questions, prior breach reporting details, and framed scenarios from both a loss and gain perspective.

Models using multivariate logistic regression for analysis for each particular dependent variable are necessary as there are multiple categorical dependent variables. The dependent variables are the Privacy Officers' responses to whether or not they would report a breach in response to prompts provided through the survey. The control and independent variables consist of categorical and continuous variables. These include demographic variables (i.e., age, gender, level of education, credentials, current employment information) and previous breach history factors (i.e., number, size, impact). Furthermore, post regression testing for predicted probabilities was conducted and the results presented display the average predicted probabilities calculated using the regression results.

A pilot study of the AHIMA Engage website for accessibility of the population determined the feasibility of the study. AHIMA Engage is a networking site which houses a member directory. AHIMA members are listed and classified by their account profile. The initial review of the site found 479 individuals with a Privacy designation in their job title.

Organization of Chapters

Chapter two of this paper details the findings from the literature review which includes the background and history of privacy in healthcare as well as information regarding the federal policies to date. Chapter two also covers the theoretical framework through its iterations over the years and then applies it to the problem of privacy breach determination, including the creation of a conceptual model. Chapter three provides information about the methodology used for the study, including the study design, population and sample parameters, survey creation, and details about the analytical methods applied. Chapter four provides the results of the analyses and interprets the findings. Chapter five discusses the hypotheses and research questions, the

theoretical and practical contributions, the public affairs implications, limitations of the study and areas for future research.

CHAPTER TWO: LITERATURE REVIEW

This literature review comprehensively details the history and background of privacy laws within the healthcare industry up through the HITECH Act/Omnibus Rule, including where they are strong and where they fall short. The chapter discusses relevant research around how the privacy laws impact healthcare facilities and whether those facilities then ensure or fail to protect patient privacy. Finally, the chapter introduces Prospect Theory and proposes its application to understand better how Privacy Officers, as agents of healthcare facilities, make decisions that ensure or fail to ensure patient privacy.

Privacy Policy

This section provides an overview of the history and background of patient privacy laws within healthcare, including areas of strength and weakness, and demonstrates its importance as a public affairs topic.

Inception of HIPAA

The United States government defined healthcare privacy and access to information as a social issue when it passed the HIPAA federal legislation in 1996 (LaTour & Eichenwald-Maki, 2006). It was a groundbreaking piece of legislation for the healthcare industry and the nation as a whole. HIPAA's purpose is to, among other things, safeguard the PHI held by a covered entity (CE) and their business associates (BA) including protecting PHI from unauthorized disclosures, otherwise known as breaches (LaTour & Eichenwald-Maki, 2006; Collins, 2007). The legislation defines PHI as any individually identifiable piece of information, whether it is oral or recorded, that contains one or more of 18 identifiers including name, date of birth, social security number, address, account number, and health plan numbers among others (California Office of

Statewide Health Planning and Development, 2015). Covered entities (CEs) are defined as healthcare providers (hospitals, physicians, etc.), healthcare plans (insurance companies, company health plans, government programs), and clearinghouses (processes data for providers and plans) (U.S. Department of Health and Human Services, 2011b).

Business associates (BA) are official contractors for CEs who perform functions for the business but are not employees of the organization (Oachs & Watters, 2016). If the BA handles PHI on behalf of the CE, they are then subject to all of the security rules under HIPAA as well as some of the privacy rules. All BA – CE relationships require a business associate agreement (BAA) that outlines the accountability of the BA to the CE including a network and user agreement and auditing procedures (Kim, Browe, Logan, Holm, Hack, & Machado, 2013).

Once HIPAA passed in 1996, covered entities needed to make sweeping changes; the handling of patient information is now of great concern. Collins (2007) identified that a crucial item lacking in HIPAA was the ability to enforce the rights and responsibilities it had established. There was no mechanism to force reporting of violations to individuals, so patients were not aware of violations of their personal information. The author stated that the legislation did not provide recourse for patients who had their privacy violated. The legislation was thus labeled as "Toothless HIPAA" (Collins, 2007).

An individual could file a complaint with the Department of Health and Human Services (DHHS), but the legislation did not compel the agency to act and they rarely investigated or imposed fines (Collins, 2007). Patients were only able to have recourse through lawsuits classified under other means including common law torts for invasion of privacy and breach of confidentiality. This was a complicated process, and as years have passed, various judgments

have chipped away the ability to successfully bring a lawsuit to fruition (Collins, 2007; Winn, 2002).

State laws attempted to fill the gap in specific areas, but as of 2001, 35 out of 50 states had a Right of Access clause, and only 6 out of 50 had a Right to Amend clause regarding hospital records, the numbers were even less for physician records (Pritts, 2002). The Right to Amend enables patients the ability to request an amendment to their PHI from a CE (Oachs & Watters, 2016). There was a need to provide an impetus for healthcare organizations to uphold HIPAA requirements through new legislation.

Defining a Breach

In 2009, President Obama passed the American Recovery and Reinvestment Act (ARRA) to help stimulate the economy. The Healthcare Information Technology for Economic and Clinical Health (HITECH) Act was a portion of ARRA and focused on 'Breach Notification'. Under these guidelines, a healthcare organization must notify patients and the Office for Civil Rights (OCR) of instances of breached PHI (Warner, 2013).

The Department of Health and Human Services (DHHS) newly defined breaches, specifically in terms of healthcare information. Reportable breaches are instances where there has been an "acquisition, access, use, or disclosure of [Protected Health Information] in a manner not permitted by the HIPAA Privacy Rule which compromises the security or privacy of the [PHI]" (U.S. Department of Health and Human Services, 2011a, p.2).

Privacy Officer Designation

The federal legislation, Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules (2013), instituted that all CEs are required to have a designated

privacy official to develop and implement the facility's privacy/security policies and procedures The specific legislation language only discusses a privacy official in terms of being responsible for the P&P development and implementation, there is a separate bullet point that the facility must have a designated contact person for handling complaints and investigations It is important to note that the legislation itself has many standards for facilities to implement, however the only personnel designation comes from 164.530 *Personnel designations* with the language outlined above (Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules, 2013). However, many facilities and studies view these positions as interconnected as they are under the same header in the legislation. The industry has identified this role as a Privacy Officer.

Liginlal and colleagues (2012) identified this individual as responsible for creating, maintaining and enforcing internal policies and procedures that align with HIPAA. Additional responsibilities include identifying breaches of PHI, determining if they are reportable and if so reporting the breach to the oversight body (Liginlal et al., 2012). There are sample job descriptions to help create or outline the responsibilities of this position. Two notable examples come from a Sample (Chief) Privacy Officer Job Description from the Privacy and Security Council (2015) and from the *Introduction to Health Information Privacy and Security* textbook by Laurie Reinhart-Thompson (2013). Both include a general purpose statement which states the Privacy Officer is responsible for the organization's Privacy Program, implementation and maintenance of the facility's P&P, and compliance with the program. Both sample job descriptions state a Bachelor's degree in health information management or other related field would be required. A Certified in Healthcare Privacy and Security (CHPS) credential and/or a

Registered Health Information Administrator (RHIA) or Registered Health Information Technician (RHIT) credential are recommended in both sources. The descriptions both identify integrity as a key skill or requirement. A final note on the job descriptions from both sources state that the name of the position may vary but that "privacy officer" is specifically mentioned in the HIPAA regulations. (Reinhart-Thompson, 2013; AHIMA Privacy and Security Council, 2015). However, as shown above, the legislation makes mention of the "privacy official," but does not outline any requirements for the position including education, skills, or credentials. Any suggested requirements for the position of Privacy Officer have come from industry.

Harm Threshold

When the HITECH portion of ARRA passed, it introduced the concept of breach notification to federal law. There was a specific definition in which this notification must occur when it posed "significant risk of financial, reputational, or other harm to the individual" (Blustein & Lapidus, 2010, para. 2). In order to require notification to the patient and OCR, the risk of harm must cross that threshold; thus the healthcare industry adopted the term 'harm threshold' (Dimick, 2010; Vinson, 2011). The legislation required a risk assessment with a focus on the harm threshold.

Assumed Risk

Those required to follow the guidelines in the healthcare industry considered the 'harm threshold' language and functionalities of the breach process vague. Therefore, after an open comment period, the Omnibus Final Rule passed in 2013 (Warner, 2013). This ruling implemented in January 2013 and went into effect September of 2013 (Wilder, Bennett, Bianchi & Peters, 2013). The term 'assumed risk' is the key change to the breach classification of

reportable as opposed to the 'harm threshold' (Bendix, 2013). When a breach occurs, a facility must assume that there is harm to the patient unless, after completion of a four-factor risk assessment, they can prove that there was sufficient low probability of compromise to the information (AHIMA, 2013a; AHIMA, 2013b). The four factors take into account:

(1) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification.

(2) The unauthorized person who used the PHI or to whom the disclosure was made.

(3) Whether the PHI was actually acquired or viewed.

(4) The extent to which the risk to the PHI has been mitigated (Terry, 2015).

While this specific terminology and the four factors may seem like a standard at the federal level for determining if a breach is reportable, it can leave organizations open to their own interpretation. Patients and their privacy are now subject to internal determinations made by healthcare organizations, which could cause significant harm if not handled appropriately.

For example, Factor (1) should take into account whether generic or sensitive information was involved; this includes mental health, substance abuse, human immunodeficiency virus (HIV), cancer, genomic, or other related information (AHIMA, 2013a; AHIMA, 2013b). For Factor (2), the recipient may have been someone with a legal obligation to protect patient information such as another covered entity or business associate (AHIMA, 2013a; AHIMA, 2013b). Factor (3) is currently under debate regarding ransomware. Finally, Factor (4) the facility can try to retrieve the information or ask that it be destroyed according to HIPAA standards. All of these steps are laden with areas where Privacy Officers are making decisions,

which can lead to vulnerability to the patient. The Patient Harm section discusses these vulnerabilities in greater detail.

Reporting Requirements

Under the HITECH Act and the concept of breach notification, organizations are required to notify outlined entities within a specific period of time. If a breach involves the information of 1 to 499 people, then an organization is required to notify the individual within 60 days of the breach and the Office for Civil Rights within 60 days after the end of the year. If a breach involves 500 people or more the organization is required to notify the individuals within 60 days, the Office for Civil Rights within 60 days, and must provide notification to 'prominent media outlets' within 60 days (U.S. Department of Health and Human Services, 2011a).

The 2009 HITECH Act requires that breaches have associated penalties in order to enforce compliance with the regulations. They occur when an organization has a breach due to not following the privacy and security guidelines, and corrective action did not occur after the incident (Holloway & Fensholt, 2013). This does not have to be the case for the future but is the established pattern so far.

The Secretary of Health and Human Services is required to make an annual report to Congress about the status of breaches and the penalties that were imposed. The first report made available covered the period after implementation, September 23, 2009 to December 31, 2010. During this period, there were 252 cases of a breach affecting 500 or more patients, which involved 7.8 million individuals. There were 30,521 cases of a breach affecting 1-499 patients, which involved over 50,000 individual patients (U.S. Department of Health and Human Services, 2011a).)

The most recent report from August of 2016, covers the calendar years of 2013 to 2014, showcases the higher number of reported privacy breaches. During this period, the numbers of breaches involving 500 or more patients were 571 cases affecting 26.5 million individuals. There were 86,707 cases involving less than 500 patients at a time, which affected 466,477 individuals (U.S. Department of Health and Human Services, 2016).) It is notable that the prior period covered only a little over a year after HITECH went into effect, and this most recent period included time after the Omnibus Final Rule went into effect.

HIPAA rules and regulations are complex, but as witnessed by the number of breach reportings over the past few years, they are necessary. Prior research noted areas where the regulations failed to protect patient privacy, and the federal government acted upon those with the creation and evolution of the HIPAA legislation. While healthcare facilities are making great strides towards protecting patient privacy, there are still many cases where they are unable to provide protection. A recent study found while facilities may take steps to protect privacy, including the use of advanced information technology systems along with biometric and two-factor security systems, breaches still occur with paper and electronic records (Gabriel, Noblin, Rutherford, Walden, & Ward, 2018).

Individual facilities determine when reporting of these cases to the patients and the federal government is necessary. While the guidelines are in place, some issues may influence decisions outside of the four-factor risk assessment. These issues can include past history with breaches, current trends, and financial liability. Patients are at risk for harm if the organization and the Privacy Officer make the wrong decision.

Factors Influencing Breach Reporting

This section reviews the relevant research around how the established privacy laws impact healthcare facilities and whether those facilities then ensure or fail to ensure patient privacy. The majority of the literature on patient privacy in the healthcare industry discusses the impact of a breach on an organization, as well as the breakdown of the causes of breaches, but there are gaps within the literature. These gaps include how the language for reporting requirements will affect the number of breaches reported to OCR and what impact an increased effort on reporting will have on healthcare entities.

Breach Types

Breach type can affect all four aspects of the risk assessment required under HIPAA. The type of breach can influence the information that was in the chart, if it was accessed, if it could be mitigated, and if an unauthorized person accessed it. OCR's reporting mechanism divides breaches into specific types. The types available are theft, loss, unauthorized access/disclosure, improper disposal, hacking/IT incident and unknown/other (U.S. Department of Health and Human Services, 2016).

Due to its accessibility on the OCR website, dissection of reported breach data of cases involving 500 or more individuals is available numerous times in the literature (Kroll Advisory Solutions, 2012; Wikina, 2014; Bai, Jiang, Flasher, 2017). It is notable that statistical analysis by third parties is lacking on data breach information involving less than 500 patients per case, as OCR has not made this data available.

For years 2013-2014, the highest percentage of breaches fell under the theft category. However, this is a downward trend as the percentages for theft have dropped from 60% in 2009

to 38% in 2014. The other categories fluctuate with 'other' being the second most common type in 2014. Unauthorized access/disclosure rose every year but one with the third highest percentage now at 26%, and it came in highest for 2014 for the number of individuals affected (U.S. Department of Health and Human Services, 2016).

Breach Causality – Human Error

Studies in the past have focused on the causes behind the errors that result in privacy breaches. (Kraemer & Carayon, 2006; Wood & Banks, 1993; Liginlal, Sim, & Khansa, 2009; Liginlal et al., 2012). Liginlal (2009) found that human errors tend to fall into one of two categories, slips and mistakes. The study identified errors as slips when individuals complete the correct action but fail to execute it accurately. Examples of slips are accessing the wrong patient chart, misdial when faxing patient information, and accessing data through unsecured methods. The study also identified that mistakes are when individuals accurately execute the wrong action. Examples of mistakes are accessing the wrong type of information within a chart and stolen or lost laptop with unsecured data (Liginlal, 2009).

An organization can continue to find answers to issues that cause many types of errors; however, studies have shown that human error is hard to eliminate (Kraemer & Carayon, 2006; Wood & Banks, 1993; Liginlal et al., 2009; Liginlal et al., 2012). In a comparison of the causes of breaches, Liginlal et al. (2012) showed that organizational privacy officers perceived that their percentage of breaches occurring from human error versus other factors was very high. It is essential to understand the different ways an error occurs to help mitigate the causing factors, but an organization must be cognizant that certain human errors will occur regardless.

Cybercrime & Ransomware

Human errors are not the only threat to the safety of patient privacy. New studies have shown that there has been a shift from primarily internal causes of breaches to external (Ponemon, 2016). The Federal Emergency Management Agency has identified external attacks, such as cybercrime and ransomware, as an area of emerging concern (Blanke & McGrady, 2016). While federal assistance is being determined, with HHS potentially collaborating with the Department of Homeland Security (DHS) and The National Institute of Standards and Technology (NIST), they have not issued formal guidance. This means facilities are still trying to understand and mitigate risk on their own (Frank, 2016).

Cybercrime has been an emerging threat as healthcare entities are vulnerable with the widespread use of electronic health records and the proliferation of networked systems (Kruse, Frederick, Jacobson & Monticone, 2016; AHC Media LLC, 2016; Blanke &McGrady, 2016). Cases of cybercrime typically involve theft of medical records for a multitude of reasons that could include identity theft or medical fraud, which is detailed in the Patient Harm (Kruse et al., 2016).

A specific area of concern is ransomware. The Office for Civil Rights defined ransomware as:

> …a type of malware (malicious software) distinct from other malware; its defining characteristic is that it attempts to deny access to user's data, usually by encrypting the data with a key known only to the hacker who deployed the malware, until a ransom is paid. After the user's data is encrypted, the ransomware directs the user to pay the ransom to the hacker … in order to receive a decryption key. (U.S. Department of Health and Human Services, 2016, p.1).

While there has been a significant amount of peer-reviewed research into cybercrime, ransomware is still relatively new. A systematic literature review of these concepts in 2016

yielded mostly news articles, with few journals producing peer-reviewed research on ransomware to date (Kruse, Frederick, Jacobson, and Monticone). This is an emerging profitable business venture for hackers, to gain access to a medical organization's system and restrict access to the organization itself in exchange for ransom (Eisenmann, 2009). This specific type of breach has been under question by the industry to determine if it is reportable, because due to its nature it would affect a large number of individuals. OCR issued unofficial guidance stating that it would be a "fact specific determination" (U.S. Department of Health and Human Services, 2016, p.7). In cases of ransomware, the hacker may disable a computer or system from usage until the organization pays the ransom, which does not necessarily mean the hacker accessed information on the device/system. Therefore, OCR recommends a fact specific-determination rather than a rigid definition. However, this leaves it open for interpretation by the healthcare facility and Privacy Officer. Breaches can occur on a variety of fronts and may be hard to anticipate, leaving facilities to be reactive rather than using a proactive prevention model.

Financial Effects of Privacy and Breaches

Privacy has a considerable financial impact on healthcare organizations. Every layer of privacy, from prevention to mitigation, can have an impact on the bottom line of a healthcare facility. A breach of patient information can be detrimental to an organization, through direct costs (penalties, lawsuits) as well as indirect costs such as lower revenue due to decreased market share (Khansa et al., 2012; Ponemon Institute, 2016; McMillan, 2015; Boerner, 2010). The financial impact a privacy breach incurs on an organization could be substantial to a larger organization and possibly even fatal to a smaller organization. Due to these factors, it is crucial to understand how healthcare organizations are reacting to the policy.

Prevention & Front-End Costs

Ideally, if asked about the need for healthcare organizations to protect patient privacy, all facilities might agree. However, there are significant upfront costs, those associated with prevention and protecting patient privacy, as required under HIPAA. When first introduced, estimated costs to implement HIPAA protections included education strategy and assessment, program management, governance, electronic transaction line items, security line items, and privacy line items all adding up to a range of $10,000 for a physician group practice to $14 million for a large integrated system (Coate & MacDonald, 2002).

The HITECH Act had requirements for covered healthcare facilities to not just implement electronic health records but to implement systems that worked in such a way that provide meaningful and securely used data (LaTour & Eichenwald-Maki, 2013). While the federal government provided funding as an incentive for meeting Meaningful Use criteria, the monetary amounts were not necessarily enough to offset the costs of implementation (Fleming, Culler, McCorkel, Becker, & Ballard, 2011). Fleming et al. (2011) found that the cost for implementation of a system that would meet meaningful use in the first year alone would be $162,000 with an additional $85,500 in maintenance fees for a 5-physician practice. Adler-Milstein, Green, and Bates (2013) in a pilot study found that only 27% of physician practices would have a positive return on investment after five years.

These studies are not taking into account the fact that Meaningful Use criteria have changed as it evolved from Stage 1 through Stage 3, and that a system installed during Stage 1 may not be sufficient to meet Stage 3 criteria. This could require significant financial requirements to meet the new standards. HITECH and the Omnibus Final Rule have added to

the financial upfront amounts by requiring expanded IT costs (security needs, system maintenance, software upgrades), legal costs (counsel, consultations), and manpower costs (update policy and procedures, privacy officer status, risk assessments) (McMillan, 2015).

These costs are critical to understand as they affect the viability and potential profitability of an organization. A study conducted by Khansa et al. (2012) found that there is a close relationship between the announcement and implementation of HIPAA standards and the fluctuation of a company's stock prices. When looking at the time directly after an announcement about a change in HIPAA requirements, there was a statistically significant negative return on a traded company's stock price (Khansa et al., 2012).

OCR Fines

Backend costs, those incurred due to a reportable breach of information can be just as impactful to the financial viability of an organization. These costs may include internal investigation, notification, OCR fines, loss of market share, damage to a brand, and potentially lowered reimbursements (McMillan, 2015).

Follow-up on reported breaches by OCR is required under HIPAA, and OCR has handed sanctions out. Since the inception of HITECH, the fines have been solely on instances where the breach affected more than 500 individuals. As of January 2, 2013, they have imposed fines on smaller breaches (Heubusch, 2011). On that date, the first settlement involving less than 500 patients occurred to the Hospice of North Idaho in the amount of $50,000 due to the theft of a laptop. HHS publicly announced it through a press statement on their website (U.S. Department of Health and Human Services, 2011b). Table 1 outlines the penalties for noncompliance.

Table 1: Penalties for Noncompliance

	Per Violation	Identical Violations / Per Year
Unaware of Violation	$100	$25,000
Reasonable Cause	$1,000	$100,000
Willful Neglect-Corrected	$10,000	$250,000
Willful Neglect-Uncorrected	$50,000	$1,500,000

Source: Modifications to HIPAA, 2013; Holloway & Fensholt, 2013

As Table 1 shows, the lowest penalty occurs when a healthcare facility is unaware of a violation, and the fine is only $100 per violation. An example of this would be if a facility had proper policies and procedures in place and the privacy breach occurred by an employee who followed the policies and procedures and had a simple mistake like a misdialed fax number. The penalties increase as the scale of the offense increases. The highest penalty is associated with Willful Neglect – Uncorrected. One example here would be a healthcare facility that completely disregards HIPAA Privacy and Security requirements with no policies and procedures, which leads to a breach of information. Another example would be that an employee steals patient information and sells it to a third party; the facility discovers the breach and does nothing to correct or mitigate the cause.

HHS publishes a list of breaches involving 500 or more patients on their website, which is accessible for anyone to see (Boerner, 2010). They have posted a list of notable breaches, as well as the action the organization has taken and the sanctions imposed on them (Boerner, 2010). Table 2 lists some examples.

Table 2: Breach Examples Involving 500 or More Patients

Date	Organization	# Patients Affected	Breach	Penalty
8/14/13	Affinity Health Plan Inc.	344,579	Leased copiers returned without wiping hard drives	$1,215,780
7/11/13	Wellpoint Inc.	612,402	Weakness in internet database	$1,700.000
5/21/13	Idaho State University	17,500	Incorrectly disabled firewall	$400,000
1/9/17	Presence Health	836	Untimely reporting of breach	$475,000
11/22/16	University of Massachusetts	1670	Malware infection	$650,000

Source: U.S. HHS, 2017

As shown in Table 2, the number of patients affected by breaches can vary in range but can be quite high. Affinity Health Plan, Inc. services healthcare plans for companies that provide health insurance to their employees. Their breach, returning leased copiers without wiping hard drives, was a common error many healthcare facilities made early on. Common knowledge in the industry seemed to miss that there are hard drives on copy machines that have the ability to store large amounts of scanned or copied data. Another example, Idaho State University, had a security issue where their firewall had been incorrectly disabled leading to vulnerabilities in the system of 17,500 patients (U.S. HHS, 2017).

Breach Costs

Costs associated with breaches are high. A study by the CSI Computer Crime and Security Institute stated that the average cost to a company for a security breach is $234,000. When factoring in the study performed by Kroll Fraud Solutions, which found that overall

5,306,000 individuals have had their privacy information breached, the numbers add up very quickly (Khansa et al., 2012).

Studies have shown the high costs associated with breaches. The Ponemon Institute (2016) conducted a benchmark study, which estimated the cost of patient data breaches annually for healthcare organizations at $6.2 billion. This study spans numerous years and is now on its sixth iteration. The study also found that of organizations that responded, 90% experienced a breach incident over the course of 2 years previous to the study and estimated cost to each organization was more than $2 million (Ponemon, 2016). These figures have held steady across all six iterations of this study, from 2010 to 2016 (Ponemon, 2012; 2013; 2014; 2015; 2016).

They also studied the economic impact of a single lost patient on the organization when considering market share, which is an average lifetime value of $113,580 per patient (Ponemon, 2016). Further studies encompassing the entire market, not just healthcare; have addressed the economic impact of data breaches on market value and shareholders, concluding that breaches concerning confidential data have a negative impact (Campbell, Gordon, Loeb & Zhou, 2003; Khansa & Liginlal, 2009; Andoh-Baidoo & Bryson, 2006; Andoh-Baidoo, Amoako-Gyampah, & Osei-Bryson, 2010).

From all of this research, it is clear that back-end privacy costs may have a sizeable financial effect on an organization. A breach of a patient's information can be detrimental to an organization as well through direct costs (penalties, lawsuits) and indirect costs such as lower revenue due to decreased market share. The financial impact of both the front-end and back-end costs on an organization could be substantial, possibly even fatal to a smaller organization.

Economic Supply & Demand

Rice and Unruh (2016) stated that the concept of supply and demand is central to the discussion of economics, where supply is the "amount of goods and services firms wish to sell at alternative prices" and demand is "how many goods and services are purchased at alternative prices" (p. 179; p. 59). The key factor stated by the authors is that supply and demand economic reasoning only holds up under a truly competitive marketplace. The authors also state that many have tried to impose these concepts onto the healthcare market in the United States without first realizing that the healthcare market in the U.S. is not truly competitive in economic terms. Of the 14 assumptions listed by Rice and Unruh that are required for a truly competitive market, the healthcare field meets few (2016).

Squire and Anderson (2015) found that the United States, as a nation, spends a great deal on healthcare, more so than other industrialized nations. The authors also found that in 2013, 17.1% of the gross domestic product (GDP) was spent on healthcare services with a per person average of $9,086. There are significant pushes to decrease the cost of healthcare as the high rate of spending has not led to better outcomes (Squires & Anderson, 2015). Cost cutting can come from a variety of avenues, and one significant area is reimbursement to medical facilities as they can conform through competitive market methods. However, as healthcare does not hold true to a competitive marketplace, this thinking can lead to dangerous consequences in patient care including the potential to jeopardize patient privacy.

If privacy is a good, and the healthcare market was truly competitive, patients would be able to demand privacy. If the facility does not supply privacy, meaning they suffered breaches and violated HIPAA rules and regulations, the patients would then be able to take their business

elsewhere. However, we have already stated that healthcare is not a truly competitive market, so what drives privacy adoptions among healthcare facilities? While there are federal rules and penalties associated with breaking them, are they enough to offset the lack of market responsiveness?

Do patients' make a choice among their healthcare facilities? This is an important question because if they are unable to purchase from another facility, does the original facility have any impetus to provide the good the patient is seeking. With the high upfront costs and the need to perform cost-cutting measures, healthcare facilities may not wish to fund privacy measures and deal strictly with the back-end breach costs, especially if it may not hurt their market share. Healthcare facilities may also choose not to report a breach since the law does leave certain decisions to the discretion of the facility to avoid the back-end costs of the breach. According to economists, demand is the key factor in a truly competitive marketplace (Rice & Unruh, 2016). However, demand may be the key factor missing to make healthcare facilities enact required privacy measures.

Patient Harm

The critical concerns for privacy breaches in healthcare are the detrimental effects for the patient, which can range from simple financial fraud, to blackmail, to medical identity fraud. In order to understand the magnitude of this issue, we must first understand why a patient having his/her privacy information breached is harmful.

Massive breaches that occur in other industries can provide prime examples. The media widely covered the Target breach. Hackers were able to access data on the credit cards of 40 million customers. The hackers may have accessed the personal information on upwards of 60

million individuals (Dezenhall, 2015). Over the next six months, other large retailers suffered breaches including Home Depot and JP Morgan Chase (Kerr, DeAngelis, & Brown, 2014). In these cases, the type of information accessed is mainly financial (Korolov, 2015). Individuals may have their credit card numbers used for false purchases and cash withdrawals leading to financial instability (Korolov, 2015; Martin, Borah, & Palmatier, 2017)

In an article by Greene (2015), cases like the Target breach where financial and demographic information was breached, significant harm comes from identity theft. Greene also stated that this differs with information stolen from a healthcare entity, which could include everything necessary to complete an identity-theft kit but with more harmful life-jeopardizing possibilities. With information including social security numbers, employment information, and birth dates, an unauthorized user can continually open new lines of credit instead of accessing just one account or one credit card (Greene, 2015).

Medical records contain extremely sensitive information (Liginlal et al., 2012). This information includes financial data as in the case of Target, but also social security numbers, demographic information, and clinical information including medical diagnoses and treatment plans (Liginlal et al., 2012).

A breach in this area can leave an individual vulnerable to a single unauthorized user, and even possibly to the world depending on how that information is used. Not only do victims need to worry about monitoring their financial statements, but they must also brace for a potentially more harmful fallout from their medical information made public or used against them (Liginlal et al., 2012).

Another potentially harmful effect to the patient is that of insurance fraud and medical identity theft (Korolov, 2015; Federal Trade Commission, 2010). The unauthorized user can expend the patient's available services leaving the patient having to pay out of pocket for critical health care needs (Korolov, 2015). This often occurs with prescription medications (Korolov, 2015). The unauthorized user can also receive treatment, which ends up on the patient's record as the patient's history (Korolov, 2015; Amori, 2008). When the patient attempts to receive medical services, the unauthorized user's treatment is intertwined with the patient's previous medical history (Korolov, 2015). The patient may also receive large medical bills for procedures and treatments incurred by the unauthorized user leading to financial loss (Amori, 2008).

Technology is advancing at a rapid pace, but it is essential to stop and consider the effects these advances might have on patients. Genetic information provides a wealth of knowledge and is extremely valuable for research purposes which is why it is a popular type of data for crowd-sourcing discoveries. Some studies have shown this type of data can be re-identified, and once available online can become immune to redaction attempts, this can be especially true in cases of genetic information with Direct to Consumer testing providers like 23andME and Ancestry.com (Zarate, Brody, Brown, Ramirez-Andreotta, Perovich, and Matz, 2016; Brase, 2018; Erlich, Shor, Carmi, & Pe'er, 2018). Other types of technological advances of concern are the implications of facial and radiological images (Parks & Monson, 2016) and health information exchange participation (Grando, Murck, Mahankali, Saks, Zent, Chern, Dye, Sharp, Young, Davis, Hiestand, and Hassanzadeh, 2017).

Prospect Theory & Privacy Breaches

This section provides the history and background of Prospect Theory and then discusses how Privacy Officers as agents of healthcare facilities can apply it to the problem of breach determination.

Prospect theory is a robust evolving theory that has many implications for management and healthcare. The theory evolved throughout the last 300 years from the concept of utility to Risk Theory to Prospect Theory, and some have even accepted a further iteration, Cumulative Prospect Theory (Tversky & Kahneman, 1992). In order to apply Prospect Theory, we must first understand its concepts, the possibilities, building blocks, constructs, and the relationship among these elements (Jaccard & Jacoby, 2010).

It is important to note that while the constructs have compounded upon each other, each one is still a crucial part of what we consider current day Prospect Theory. Throughout the years the research has built upon the exiting foundation, keeping the original constructs and adding new ones with each iteration. Prospect Theory has the following constructs of concepts listed in Table 3.

Table 3: Prospect Theory Overview

Construct	Definition
Utility	Satisfaction level
Diminishing Marginal Utility	As item increases, utility of increase diminishes
Risk Behavior	Risk averse, risk neutral, risk seeking
Reference Point	Individual's status on …[a] commodity
Value Function	In terms of gains= risk averse; In terms of loss= risk seeking
Weighting	Overweigh (w+, small probabilities) and Underweight (w-, large probabilities)
Framing	View of outcome will determine willingness to take risk dependent on value function
Loss Aversion	People prefer to avoid a loss rather than have a gain

Source: Arrow, 1971; Briggs 2015; Bernoulli, 1738; Kahneman & Tversky, 1979; Tversky & Kahneman, 1991

In Table 3, the theory terminology used for each construct has an applicable definition. Each construct utilizes its original authors' theory. The next section moves through the iterations of theory that led to modern-day Prospect Theory highlighting the constructs listed in Table 3

Risk

Prospect Theory can be traced back to the 1700s. In 1738, Daniel Bernoulli published a paper detailing *The Measurement of Risk* in which he used statistical principals to describe a way to measure risk without taking individual factors into account, rather than just the probability of an event occurring. Bernoulli identified the first construct of what we consider modern day Prospect Theory, utility. Utility indicates satisfaction levels. An individual will take a risk in

proportion to their utility from the outcome, their satisfaction level with the chance of gain, rather than taking into account the proportion that the gain will occur (Bernoulli, 1738).

Diminishing Marginal Utility

The theory continued to evolve when Alfred Marshall addressed it in his book *Principles of Economics* (1890). He found that additional increments of an outcome increase utility. However, utility does not increase at a consistent rate. The further removed from the initial reference point, meaning the more one has of something, the increase in utility diminishes (Marshall, 1890; Holmes et al., 2011). This is the second construct of Prospect Theory, diminishing marginal utility (Marshall, 1890).

A simple illustration of this is money. A person starting at $0 who gains $100 will have high utility. As they continue to gain in $100 increments, the utility they derive lessens. Thus, when the individual has $100,000, adding an additional $100 does not hold the same value of utility as when they had $0.

Risk Aversion Theory

In the 1960s, John Pratt (1964) and Kenneth Arrow (1971) developed a theory for what had been building to that point, Risk Aversion Theory or, in some research, Expected-Utility Theory. The theory builds upon previous works by including a classification among individuals regarding their willingness to accept risk, which is the third construct under Prospect Theory, risk behavior (Arrow, 1971). Individuals fall into one of three categories, risk averse, risk neutral, and risk seeking (Pratt, 1964; Arrow, 1971). In an individual who is risk averse, all the characteristics that were determined before hold true including diminishing marginal utility as gains increase (Pratt, 1964; Arrow, 1971). In an individual who is risk neutral, risk will make no

difference in their decision. In an individual who is risk seeking, they gain greater marginal utility with the chance of risk and as their overall wealth increases (Arrow, 1971).

In Figure 1, graphs A, B, and C show the pattern of behavior based on our fourth construct, expected utility. Dependent on the viewpoint of the individual on risk, the expected utility, or prospective level of satisfaction, changes (Arrow, 1971).

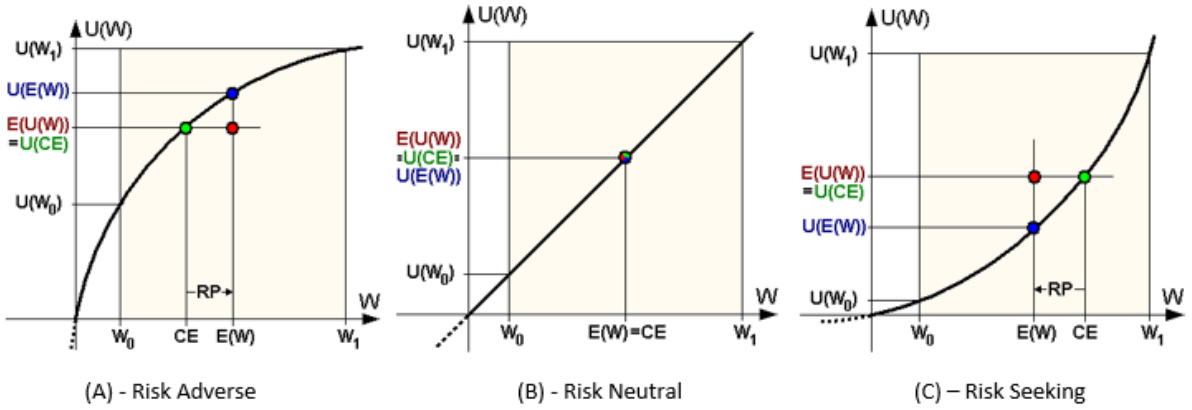

Figure 1: Risk Premium

Source: Qniemiec, used under CCO 1.0/Combined graphs

Evolution to Prospect Theory

Daniel Kahneman and Amos Tversky (1979), built upon existing risk aversion theory to create their seminal article *Prospect Theory: An analysis of decisions under risk.* They postulated that a value function is necessary as a person will use a reference point to evaluate the outcomes that are possible. Up until this point, the authors stated that it was determined that an individual would decide whether or not to take a risk based only on the amount of utility they would get from the outcome in regard to their overall wealth. With reference points, it was determined that the individual would make a decision based on the value of either gains or losses from the risk

"relative to some neutral reference point" (Kahneman & Tversky, 1979, p. 274). This influences Research Questions 1 and 2:

RQ1: Does the Privacy Officers' reference point based on knowledge levels affect their choice to report a breach of patient information?

RQ2: Does the Privacy Officers' reference points based on past reporting affect their choice to report a breach of patient information?

Kahneman and Tversky (1979) and Prospect theory brought the concept of loss into theory, no longer just determining risk based on the gain but also where loss was concerned. The authors stated that when individuals make decisions concerning both, the central graphs of risk aversion and risk seeking hold true but add together. The value function stipulates that when evaluating gains, a person is risk averse and when evaluating losses, a person is risk seeking (Kahneman & Tversky, 1979). The new graphical representation of this is in Figure 2. The risk averse behavior is on the upper right quadrant, and the risk seeking behavior is in the lower left quadrant.

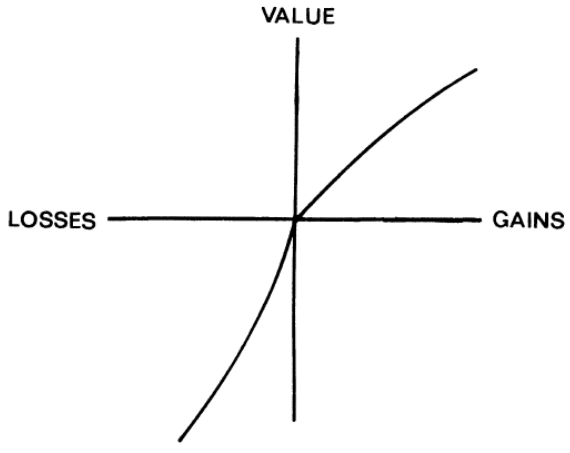

Figure 2: Hypothetical Value Function

Source: Kahneman & Tversky, 1979

Prospect theory included what Bernoulli had established in the 1700s and compounded upon it, that individuals do not use the actual probability of the risk when considering it (Bernoulli, 1738). Probability of a risk outside of absolutes, 0% or 100%, is not aligned with the decision weights given by individuals (Kahneman & Tversky, 1979; Holmes et al., 2011). As illustrated in Figure 3, individuals tend to overweight (in very small probabilities) and underweight (in large probabilities) the actual probability of their choices when deciding whether to take the risk (Kahneman & Tversky, 1979).

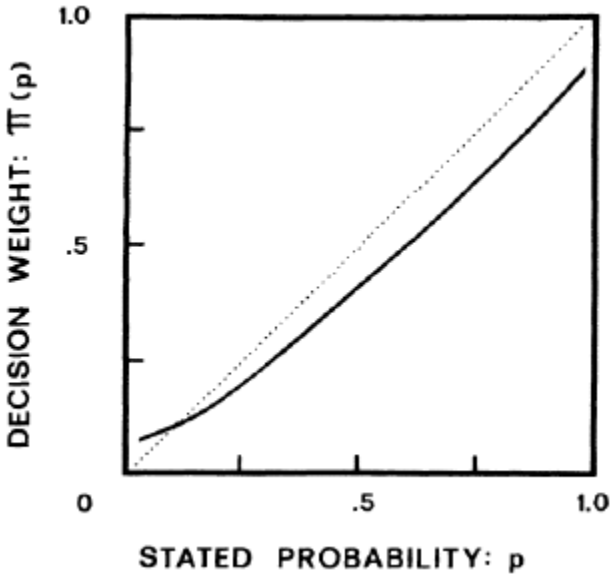

Figure 3: Probability Weighting

Source: Kahneman & Tversky, 1979

Another fundamental change from established risk aversion theory was the inclusion of framing. Kahneman and Tversky (1979) used the concept of framing to explain that the way an individual views the outcome of risk will determine their willingness to take the risk dependent on the S-shaped curve shown in Figure 2. The authors found that one person may view the outcome as a gain, which means the likelihood of the individual taking the risk falls on the risk

averse concave curve. However, another person may view the outcome as a loss, which then will lead to the likelihood of the individual taking the risk to fall on the risk seeking convex curve (Kahneman & Tversky, 1979). This influences Research Question 3:

RQ3: Does the framing of a scenario affect Privacy Officers' choice to report a breach of information?

Loss Aversion

Not even a decade after Tversky and Kahneman (1991) began writing about Prospect Theory they published another paper regarding the concept of loss aversion. This expanded upon the inclusion of the loss function to create the S-shaped curve. The authors found that on the loss side, the convex curve has a sharper steep in the beginning as opposed to the concave curve on the gain side; this is to simulate that a person will feel a loss 'harder' than a gain. Even though it has a steep downward projection in the beginning, the authors stated that the loss functions the same as a gain in that it has diminishing sensitivity. Just as utility plateaus for an individual's gain, so does the hurt from a loss (Tversky & Kahneman, 1991).

Cumulative Prospect Theory

A decade after their 1979 seminal article, and only one year after their loss aversion paper, Tversky and Kahneman (1992) were able to build upon their original model and released *Advances in prospect theory: Cumulative representation of uncertainty*, which detailed Cumulative Prospect Theory. The authors stated that the main difference between these two works is that when individuals are regarding the probabilities (and likely underweighting and overweighing them) they view these differently based on whether the risk is seen from a gain or

a loss perspective. In Prospect Theory, an individual will view the probability the same no matter the framing as a gain or a loss (Tversky & Kahneman, 1992).

As can be seen in Figure 2, the straight line is the probability of a risk-neutral individual, which means they do not distort the weights; they only view the actual probability (Tversky & Kahneman, 1992). The w+ line shows that someone viewing the risk as a gain will overweigh a low probability even more than someone viewing the risk as a loss. These same people from a gain perspective will underweight a high probability even more than someone from a loss perspective (Tversky & Kahneman, 1992).

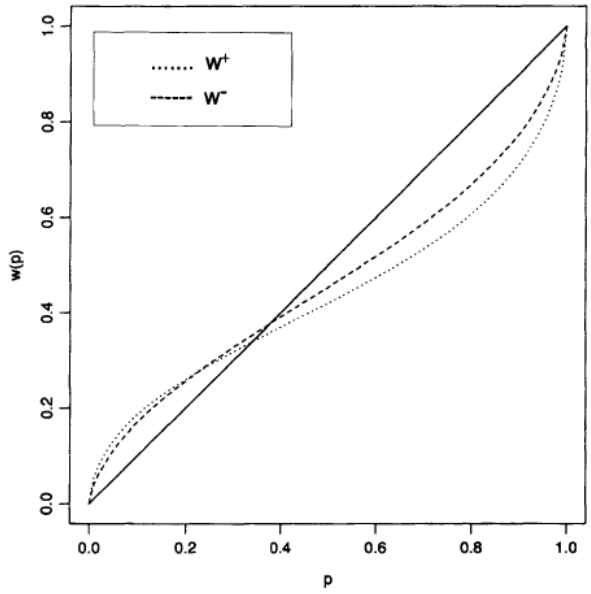

Figure 4 Weighting Functions for Gains (w+) and Losses (w-)
Source: Tversky & Kahneman, 1992

Another difference that occurs between the two theories deals mostly with the mathematics. When creating the equation for Prospect Theory the value of the gamble is a function of two outcomes, whereas in Cumulative Prospect Theory the value of the gamble "applies to any finite [gamble]" no matter the number of outcomes provided (Tversky &

Kahneman, 1992). This is important to note, as one must consider the amount of times the outcome of a risk is only a loss or a gain. Many times, it will be a combination or multiplication of the two.

Weaknesses of Prospect Theory

The changes as theory evolves may seem minute when discussing the content of the theory, but in the mathematical portion they make a significant difference. However, due to the seemingly minute changes, many researchers use the terms Prospect Theory and Cumulative Prospect Theory interchangeably, as they are accepted theories at this point. Many articles do not mention cumulative, especially if they are not formulating the actual equations and are only using the conceptual portion of the theory as will be the case in this study.

Another area of weakness when using Prospect Theory is that as it is highly mathematical with origins in economics, researchers may find it difficult to apply to social research without a mathematician. This could deter the application of Prospect Theory to multiple settings where it could prove useful. Its concepts, outlined later, are applicable to understand decision-making concerning risk in a general sense. While multiple types of settings have applied the theory, one specific study referenced a need for further research of message framing with uncertain outcomes (Evangeli, Kafaar, Kagee, Swartz, & Bullemor-Day, 2013).

Conceptual Map

The ten constructs listed in Table 3 together form Prospect Theory. Each piece builds upon the piece before. Utility is the starting point, where an individual moves through the list of the following constructs and choices begin to take shape. The process of placing constructs into a map converts the conceptual system into a symbolic expression and provides theory construction

(Jaccard & Jacoby, 2010). This signifies statements about the relationships between the concepts/constructs (Jaccard & Jacoby, 2010). The Prospect Theory conceptual map is in Figure 5.

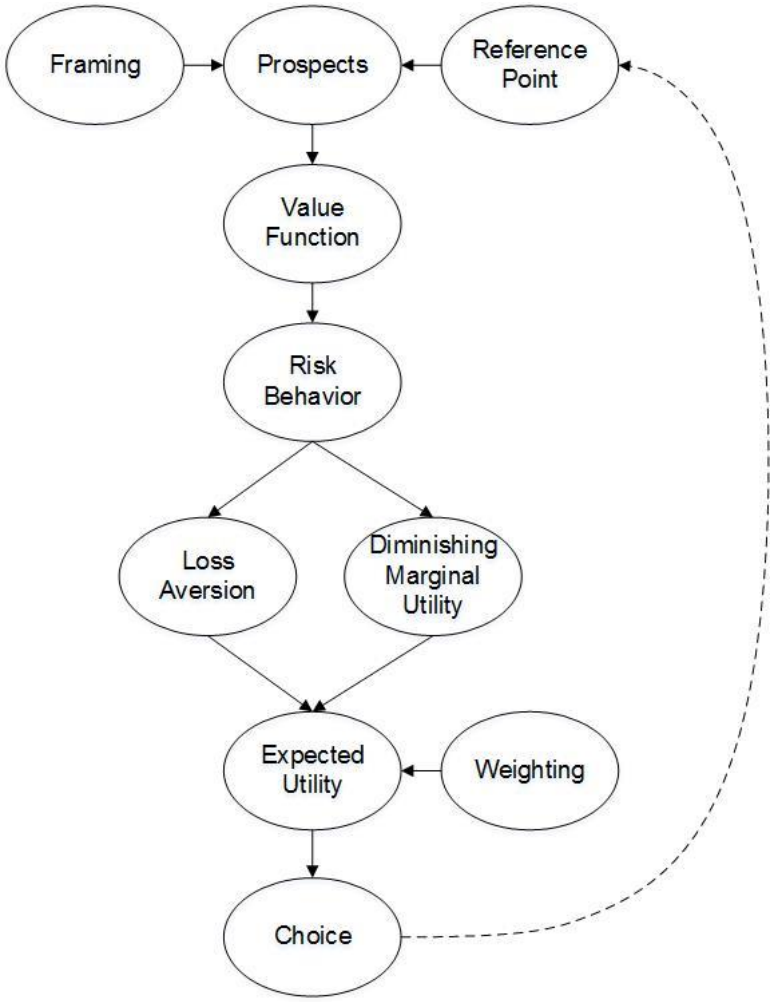

Figure 5: Prospect Theory Conceptual Map

An individual's reference point is his/her starting view for the process. Framing is a factor of choice presentation. To begin, prospects (choices) are presented. Both the frame and reference influence how the view of the prospects and what their value functions are. The value function of the choice determines the risk behavior used. The risk behavior influences the use of

loss aversion and the diminishing marginal utility of the choice. These two impact the expected utility of the prospects. The individual's weighting of the probabilities impacts the expected utility as well. From the expected utility, the individual will then make a choice. The choice individuals make then affect their new reference point for all future prospects. This conceptual map provides the basis for the choice of variables used for the study.

As the theory has been broken down into its concepts and constructs, its evolution, and can now visually map it, it is possible to evaluate it to see if it fits the standard of a good theory. This is crucial to determine if it is appropriate to utilize the theory for further academic research. To evaluate Prospect Theory, it will be compared against several criteria outlined by Daniel McCool in *The Public Policy Theory Primer* (Smith & Larimer, 2013) and by Jaccard and Jacoby in *Theory Construction and Model-Building Skills: A Practical Guide for Social Scientists* (2010).

Not all criteria listed by McCool and Jaccard and Jacoby will be used, as McCool stated that it is highly unlikely that a theory will contain every aspect. It places an undue burden on the theory to expect it to meet all the criteria listed, so if it does fall short on some points, it would not necessarily cause immediate dismissal (Smith & Larimer, 2013). Table 4 evaluates Prospect Theory.

Table 4: Evaluation of Prospect Theory

Criteria	Further Definition
Utility/Validity	Accurate representation and guide of reality
Logically consistent	Not contradictory
Scope	Encompasses a large range
Testability	Provides hypotheses
Organization/Understanding	Imposes order
Heuristic	Provides future research
Predictiveness	Model for prediction
Relevance/Usefulness	Novel insight
Reliability	Supports replication

(Smith & Larimer, 2013; Jaccard & Jacoby, 2010, p. 31-32)

The theory meets all of the criteria mentioned in Table 2. Of most importance is that the theory has utility and validity. Given the types of social problems we can address with this theory it meets this criterion. Prospect Theory also provides usable hypotheses which many researchers list as a major criterion of a good theory, especially as there are no overarching public policy theories that currently can satisfy this need (Smith & Larimer, 2013, p. 30). Therefore, when adopting theories from other fields to public policy issues, these two criteria are of great priority.

Management/Healthcare Applications

Max Bazerman (1984) found a correlation between Prospect Theory and organizations. All of the information provided previously has centered on how an individual would analyze risk and make a personal decision. However, many are taking the concepts provided in these theories and applying them to the business and healthcare fields. Bazerman (1984) made this jump and wrote about Prospect Theory, particularly the concept of framing, and how it can explain aspects of organizational behavior.

Holmes, Bomiley, Devers, Holcomb, and McGuire (2011) concentrated on the key concepts behind utility, risk aversion, prospect, and Cumulative Prospect Theory. The authors applied Prospect Theory to management concepts. They provided examples of executive compensation, negotiations, affect and motivation, and human resources management (Holmes et al., 2011). Some of these topics synthesized what was in earlier research, the impact of reference points and framing in decision-making and pay scales. They also showcased higher-level concepts that are organization level issues, organizational risk and return as well as firm risk-taking behaviors.

While this study will focus on how individual Privacy Officers make decisions regarding breach notification, it is important to understand their position as an agent of an organization. While an organization itself may not make decisions, individuals are making these decisions on behalf of the organization. Just as Bazerman found that Prospect Theory could apply to organizations, so too does it apply to Privacy Officers making decisions on behalf of healthcare facilities.

Privacy Breaches Illustrated with Prospect Theory

Federal policy must be clear and useful in order to guide organizations. Without clear guidance, healthcare facilities may view ambiguous language from their perspective, which could affect their behavior. If the behavior in response to a privacy breach is not appropriate, the patient's information is at risk, which can lead to serious financial, emotional and physical harm. This research focuses on the use of Prospect Theory to understand how Privacy Officers, as agents of healthcare organizations, act regarding breaches of patient information that are not clearly definable by the existing federal policy. This study adds to the body of knowledge as there are no previous studies that have applied Prospect Theory to decisions regarding healthcare privacy.

The scenario presented concerns privacy risks as determined by an individual Privacy Officer of a healthcare organization. Healthcare privacy can utilize the model presented in Figure 3 in many ways; however, the language ambiguity of the Breach Law will be the focus. In this case, the hypothetical facility has endured a breach. The prospects (choices) are the classification of the breach.

The reference point for a Privacy Officer begins with knowledge about the privacy laws and the status of having experienced a prior breach. The prospects are to report the breach or not to report the breach in accordance with HIPAA and the Omnibus Final Rule. The language from the Omnibus Final Rule states facilities must "assume harm" unless they can prove otherwise which makes the default choice to report. The Privacy Officer then uses the reference point to frame the prospects as a gain or a loss.

For example, in scenario A shown in Figure 6, a Privacy Officer has experienced a reportable breach before, and he/she knows the monetary consequences and harm to the reputation, so the value function is 'reporting' is a loss and 'not reporting' is a gain. The value function assigned is dependent on the organizations' reference point and framing.

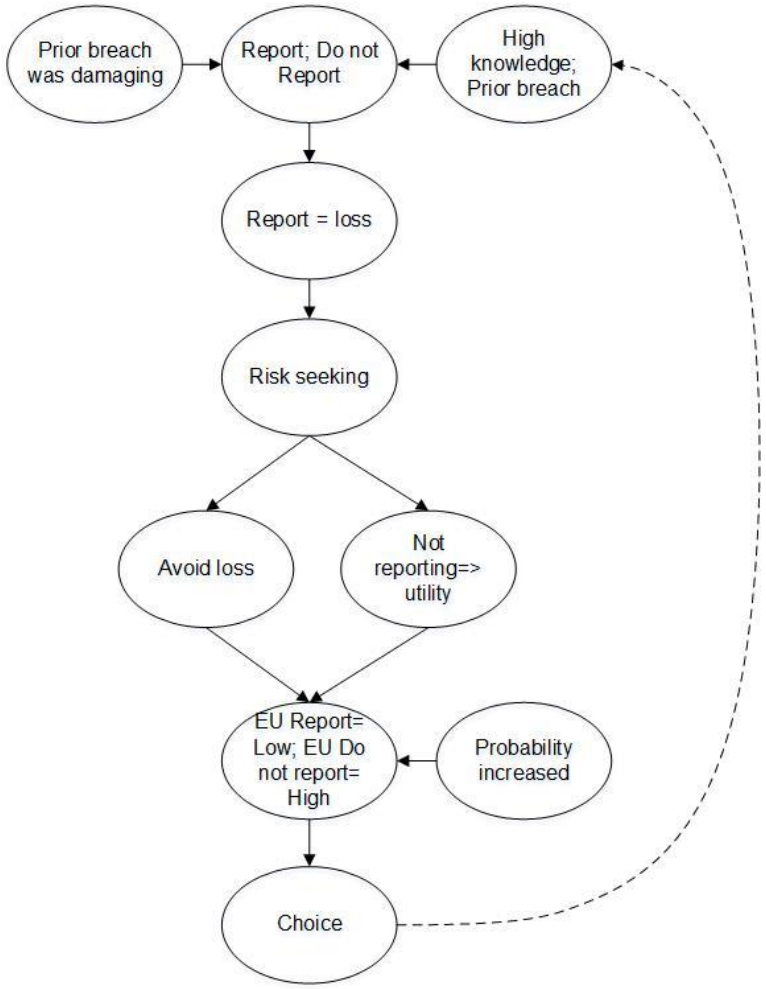

Figure 6: Prospect Theory Scenario 'A' Concept Map

Now that the Privacy Officer has determined reporting a breach is a loss he/she falls into the risk seeking behavior category. This triggers loss aversion; the Privacy Officer sees reporting a breach as a loss so he/she will do what is necessary to keep that from occurring. It

also affects the way diminishing marginal utility plays a role. A loss may be extremely hurtful, but if they keep experiencing a loss, the impact of each loss decreases.

The viewpoint of the risk from both the loss aversion and diminished marginal utility aspects then influence the expected utility of the choices. This is the utility the Privacy Officer will feel from the different prospects available given both those aspects. The Privacy Officer will also weigh the probabilities differently for the two prospects given his/her framing of them. If reporting is a loss, even though it might seem like a small probability that there might be a loss, the individual will tend to overweigh and inflate the probability in his/her mind. With the expected utility of each prospect now available with all the influences given, the organization can make what they deem the best choice. It could be the opposite, as shown in scenario B in Figure 7; an organization did not have a prior breach so 'reporting' is not a gain or a loss.

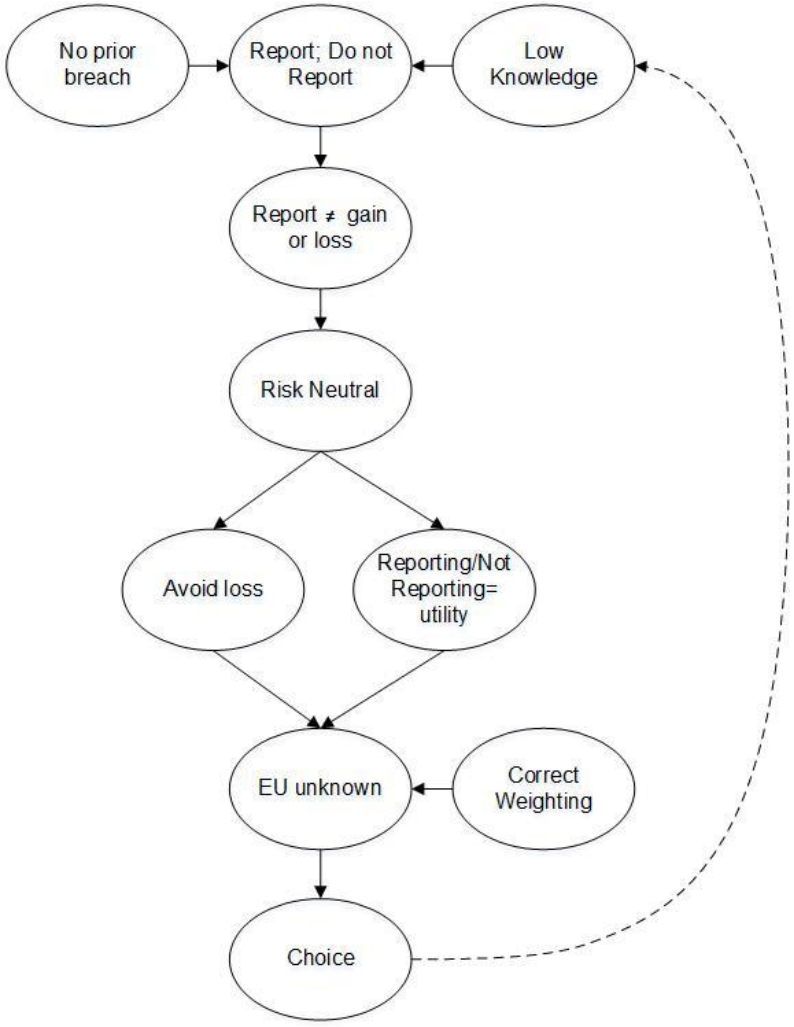

Figure 7: Prospect Theory Scenario 'B' Concept Map

A third option in Figure 8 is scenario 8, showcases an organization with a prior breach, which did not report, was audited and fined for failure to report. In this scenario, 'not reporting' is a loss and 'reporting' is a gain.

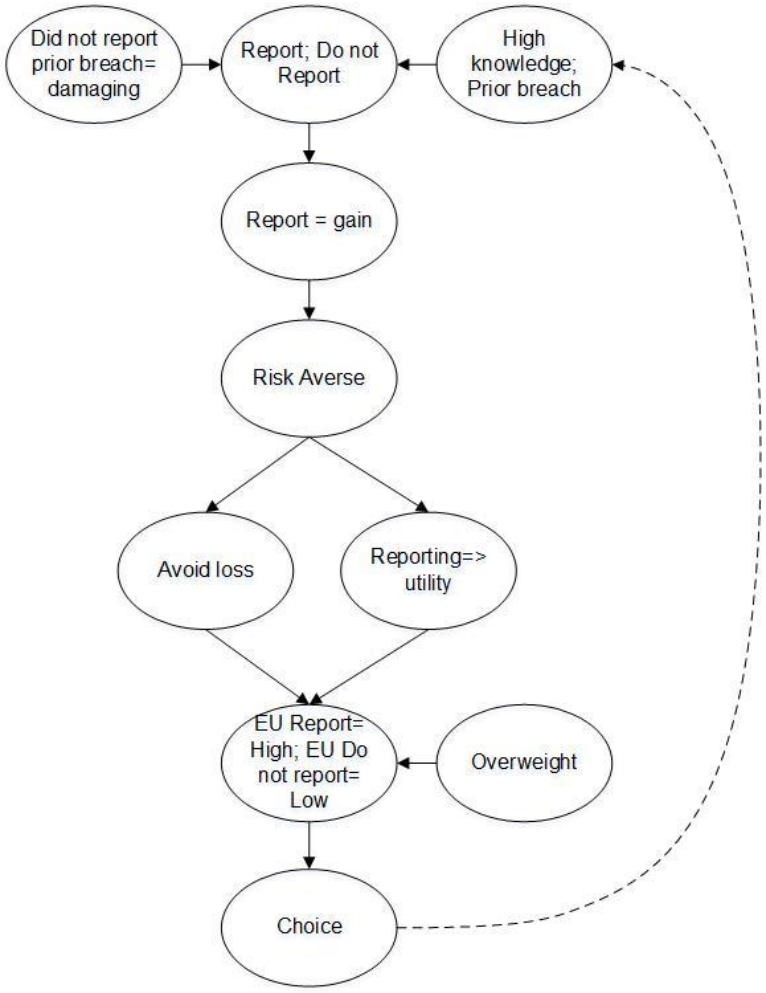

Figure 8: Prospect Theory Scenario 'C' Concept Map

The use of Prospect Theory in healthcare research is still relatively new. Individual behavior has used the theory for quite some time; however, its implications to management/healthcare analysis are wide open. This theoretical framework will help explain a Privacy Officer's view of the risk of potential privacy breaches which will then, in turn, lead to predicting the actions taken to report or not report. With the policy language open to interpretation, it places the impetus for action on the organization through their Privacy Officers, and each Officer may behave differently dependent on their experiences.

CHAPTER 3: METHODOLOGY

The following chapter outlines the research questions and hypotheses addressed by this study, discusses the research design and sampling method including data collection and measurement, and explains the data analysis methodology. To provide clarification regarding the specific variables studied and the methodology used for data analysis, the chapter organization is as follows: research questions and hypotheses; research design, sampling and measurement; data collection and analysis, and finally the ethics of the study.

Research Questions and Hypotheses

RQ1: Does the Privacy Officers' reference point based on knowledge levels affect their choice to report a breach of patient information?

H1: Higher percentage of years employed in the healthcare field is positively associated with reporting future indefinable breaches of healthcare information in a general scenario.

H2: Higher percentage of years employed in the healthcare field is positively associated with reporting future indefinable breaches of healthcare information in a gain scenario.

H3: Higher percentage of years employed in the healthcare field is positively associated with reporting future indefinable breaches of healthcare information in a loss scenario.

H4: Lower level of self-reported knowledge in healthcare privacy is negatively associated with reporting future indefinable breaches of healthcare information in a general scenario.

H5: Lower level of self-reported knowledge in healthcare privacy is negatively associated with reporting future indefinable breaches of healthcare information in a gain scenario.

H6: Lower level of self-reported knowledge in healthcare privacy is negatively associated with reporting future indefinable breaches of healthcare information in a loss scenario.

H7: Higher levels of education are positively associated with reporting future indefinable breaches of healthcare information in a general scenario.

H8: Higher levels of education are positively associated with reporting future indefinable breaches of healthcare information in a gain scenario.

H9: Higher levels of education are positively associated with reporting future indefinable breaches of healthcare information in a loss scenario.

H10: Attainment of a Certified Healthcare Privacy and Security credential is positively associated with reporting future indefinable breaches of healthcare information in a general scenario.

H11: Attainment of a Certified Healthcare Privacy and Security credential is positively associated with reporting future indefinable breaches of healthcare information in a gain scenario.

H12: Attainment of a Certified Healthcare Privacy and Security credential is positively associated with reporting future indefinable breaches of healthcare information in a loss scenario.

H13: Attainment of a Registered Health Information Administrator or Technician credential is positively associated with reporting future indefinable breaches of healthcare information in a general scenario.

H14: Attainment of a Registered Health Information Administrator or Technician credential is positively associated with reporting future indefinable breaches of healthcare information in a gain scenario.

H15: Attainment of a Registered Health Information Administrator or Technician credential is positively associated with reporting future indefinable breaches of healthcare information in a loss scenario.

RQ2: Does the Privacy Officers' reference points based on past reporting affect their choice to report a breach of patient information?

H16: Prior reporting of a breach of healthcare information to the Office for Civil Rights is positively associated with reporting future indefinable breaches of healthcare information in a general scenario.

H17: Prior reporting of a breach of healthcare information to the Office for Civil Rights is positively associated with reporting future indefinable breaches of healthcare information in a gain scenario.

H18: Prior reporting of a breach of healthcare information to the Office for Civil Rights is positively associated with reporting future indefinable breaches of healthcare information in a loss scenario.

RQ3: Does the framing of a scenario affect Privacy Officers' choice to report a breach of information?

H19: A breach of healthcare information scenario framed as a gain is positively associated with privacy officers classifying the breach as reportable to the Office for Civil Rights.

H20: A breach of healthcare information scenario framed as a loss is negatively associated with privacy officers classifying the breach as reportable to the Office for Civil Rights.

Research Design

This study utilizes primary data through a research survey conducted over a single year time period. As the study aims to gather data on a sample of a population at a single instance in time, a non-experimental cross-sectional research design is used (Babbie, 2001). This type of design is preferable due to feasibility and ethical restrictions (discussed later) that prevent conduction of a true experimental study. The collection of primary data was necessary due to a lack of prior research of this format and subject. Prior to data collection, the Institutional Review Board at the University of Central Florida completed an initial review as well as a secondary review of the follow-up email format.

This study design meets the criteria for internal validity, that the results are attributed to the study and not flaws in the design or unaccounted-for factors. As the study utilizes a cross-sectional design, maturation- as the sample ages they change, instrumentation- changes occur in the measurement instrument during pre-and post-test, and experimental mortality- as the study progresses individuals in the sample drop out, are not applicable. However, as a questionnaire with multiple scenarios is being used, testing- the questions themselves bias the answers, and experimenter-bias, could be valid threats to the study (Babbie, 2001). Steps were taken to counteract this include the use of pilot testing and subject matter experts to review the questionnaire.

Survey questionnaires in the Privacy Officer and/or breach notification area are few and not easily accessible. As there were not pre-screened surveys available it was necessary to develop a new questionnaire.

Care was taken during the questionnaire development to identify issues that could lead to threats to internal validity. When creating a questionnaire, bias or ambiguity in wording occurs. Using an outside review team, such as a subject matter expert and a pilot study, helps bring another point of view to help correct and clarify questions and format (Babbie, 2001). Pilot study participants and a subject matter expert reviewed the questionnaire for ease of use by survey participants and provided guidance on the scenarios. Extraneous and confounding variables are of major concern, as the analysis will use logistic regression. After completion of the analysis by the subject matter expert and pilot study, the feedback was reviewed to eliminate threats; more discussion of this is located in the Analysis section. The survey questionnaire is located in Appendix E.

Population & Sample

The population for this study is individual healthcare Privacy Officers affiliated with the American Health Information Management Association (AHIMA). AHIMA is a national organization that oversees the Health Information Management workforce in the United States by credentialing and membership. AHIMA has taken the lead in HIPAA and Privacy as it is part of the educational program-credentialing exams, as well as the focus of a specialized credential, the Certified in Healthcare Privacy and Security (CHPS) (AHIMA, 2017).

The focus is placed on this population of individuals for this study as Privacy Officers are required under HIPAA and are responsible for handling any breaches of health care information

that occur within a facility. Affiliation with AHIMA is critical for access to knowledge and resources as well as access to the study population.

To ensure that the sample is representative of the population, and due to the nature of the population, a non-probability purposive sampling method is used. Therefore, sampling was conducted based on specific characteristics (Babbie, 2001). The characteristics focused for this study include AHIMA membership, listing in the AHIMA Engage directory, and Privacy designation. AHIMA offers a networking site, Engage, which houses a member directory. AHIMA automatically lists the members and classifies their information by their AHIMA account profile. AHIMA members do self-select their information, including job category; however, the information must be current and accurate for credentialing purposes.

The information from Engage is not a downloadable list, and due to size constraints, searches of the list can only occur in small quantities, meaning only the first 200 results populate. Therefore, an advanced search was conducted by state and by job level, which was limited to Director (e.g., HIM IT)/Officer (e.g., Privacy). This was sufficient to limit the results per state to under 200 individuals with the exception of seven states. These included California, Florida, Illinois, New York, Pennsylvania, Tennessee, and Texas. A search by the initial letter of the last name was performed to capture all individuals for these states. Individuals identified with Privacy in their title were the only ones sent the survey questionnaire. Of note, Delaware was the only state that did not have any individuals denoted by Privacy in their title. There were six states with only one individual with a Privacy title identified. To ensure the anonymity of survey respondents, aggregation of results occurred by "state healthcare privacy notification law status."

A breakdown of the number of AHIMA members listed as Director and with a Privacy designation is located in Appendix H.

Measurement

Using individual Privacy Officers as the unit of analysis and the methods outlined above, surveys were distributed. Reliability and validity of the study are paramount, and multiple methods satisfied the four cornerstones of a quality survey as listed by Dillman, Smyth, Christian, and Melani (2014). These include: (1) coverage error – the sample does not represent the population for estimation purposes; (2) sampling error – the estimate produced by the sample is different from an estimate produced by the population; (3) nonresponse error – there is a difference in the results from the group that responded and if all of those sampled responded; and (4) measurement error – the respondents provided inaccurate responses through inability or unwillingness due to survey design (Dillman et al., 2014).

To account for coverage error, a narrowing of the study's population occurred. To account for sampling error, all members of the identified population were asked to participate. The request for participation was structured to attract all participants, which accounts, as much as possible, for nonresponse error. Development of the questionnaire occurred through discussions with the committee and members of the healthcare privacy community. A subject matter expert reviewed the questionnaire for ease of use by participants and appropriateness of scenarios. A pilot study was conducted by submitting the questionnaire to volunteer individuals with healthcare privacy experience to account for measurement error. The individuals invited to participate accessed the Qualtrics survey to account for the entire experience that survey respondents would have. An additional question at the end of the survey asked "Feedback:

Comments/Concerns on Questions – For Pilot Study." Feedback from pilot study participants is located in Appendix J.

Questions use the guidelines listed for closed-ended questions provided by Dillman et al. (2014). Areas of concern in question design that were addressed include positive and negative stems, category lists include all possible reasonable answers, mutual exclusivity present in lists, appropriate answer spaces dependent on question's intent, multiple choice or forced-question formats used where appropriate, and scale design (Dillman et al., 2014).

Data Collection

To determine the feasibility of this study, an initial examination of the ability to obtain contacts for survey distribution occurred. A review of the AHIMA Engage Directory proved time-consuming but achievable. An initial listing by state showed 5293 individuals with the Director/Officer classification, and of those 479 individuals had Privacy in their title.

A trial run of the messaging system within Engage was successful. Messages sent through the Engage system send an email to the individual's desired email address and includes the full copy of the text and functioning HTML links. This was tested to make sure that there were no additional steps or logins required in order for individuals to access the information for the study, or the link for the survey, which might hinder response rates. The system provides all the necessary information to the potential participants in an easily read, seamless manner. The most considerable burden was on the researcher sending out the messages as it was on an individual level, but it was feasible within a reasonable timeframe.

Identified AHIMA members were contacted by messaging through the Engage site. This required selection of a 'send message' box which opened up a new window where a "subject"

area was required to be filled in, as well as a "message" area. The process was repeated at an individual level for all 479 identified Privacy Officers.

Data collection utilized the University of Central Florida Qualtrics online survey tool. The message included a bitly link to the Qualtrics survey for ease of use and understanding. This minimized costs associated with this portion of the research. In order to reach a sufficient sample size, follow-up was necessary through the AHIMA Engage site as well with targeted emails. The initial email was sent on a Tuesday, a first reminder email was sent two weeks later, and a final reminder email was sent one week later. With a margin of error of 8%, a significance (alpha) level of 0.05, and a population of 479, the minimum sample size required is 115 individual responses (Raosoft, 2017). This minimum sample size enables strong conclusions and generalizability of the results (Gogtay, 2010).

The initial survey request received 85 responses from participants. As the minimum sample size required by the power analysis was 115, a follow-up was sent two weeks after the original request. From that, there were an additional 57 responses which brought the total to 142. However, an initial review of the data showed 27 responses were ineligible for the study. One final request for participation the following week resulted in 170 responses, resulting in an appropriate sample size for robust analyses (Dillman et al., 2014).

Data Analysis

Univariate, bivariate, multivariate and post regression statistics characterized the data to address the research questions and hypotheses. For research questions one and two, there are three dependent variables which use multivariate logistic regression, therefore three separate models tested the hypotheses. Post regression testing of the logistic regression models yielded

predicted probabilities. For research question three, chi-square tests analyzed the hypotheses. This section includes the analysis methodology for each set of models, the formula, the corresponding research questions and hypotheses, and finally the operationalization of variables table specific to those models.

For all regression models, the control and independent variables remained the same. The variables that occurred across all three models are control (Age, Gender, Department, State Laws, Facility Classification, and Profit Status) and independent (Years HC, Years HC Privacy, Education Level, Credentials, Knowledge Level, Prior Breach Status, Breach Number, Breach Effects). The three dependent variables are General Breach Scenario, Gain Breach Scenario, and Loss Breach Scenario.

Multivariate Analyses of Breach Reporting

Logistic regression analyzed the effect that multiple independent variables, both categorical and continuous, have on a single dependent categorical variable. This assesses the hypotheses about factors associated with reporting a breach of PHI to OCR in multiple scenarios. The general assumption required is a lack of multicollinearity, that the independent variables will not be correlated (Pallant, 2013). This will be determined using the Tolerance Factors and the Variance Inflation Factors (Pallant, 2013). To ensure a lack of multicollinearity, a test for correlation occurred. Chi-square analyses examined the relationship between the variables at an individual level. There are three separate multivariate logistic regression models, but all use the following model:

$\log y = \propto + \beta_i x_i$ where:

$\propto$= Constant
β= Regression Coefficient
x_i Stands for the following variables, both independent and control:

The research questions and hypotheses that are addressed with the multivariate logistic regression tests are as follows:

RQ1: Does the Privacy Officers' reference point based on knowledge levels affect their choice to report a breach of patient information?

Hypotheses H1-H15

RQ2: Does the Privacy Officers' reference points based on past reporting affect their choice to report a breach of patient information?

Hypotheses H16 – H18

The operationalization of the variables for the multivariate logistic regression are shown in Table 5 and Table 6.

Table 5: Operationalization of Dependent Variables

Variable	Variable Type	Variable Classification	Measure	Source	Definition
General Breach Scenario	Dependent	Categorical	Not Report=0 Report=1	Survey	Self-choice to report future ambiguous breaches to OCR
Gain Breach Scenario	Dependent	Categorical	Not Report=0 Report=1	Survey	Self-choice to report gain framed ambiguous breach to OCR
Loss Breach Scenario	Dependent	Categorical	Not Report=0 Report=1	Survey	Self-choice to report loss framed ambiguous breach to OCR

Table 6: Operationalization of Independent and Control Variables

Variable	Variable Type	Variable Classification	Measure	Source	Definition
Years HC	Independent	Continuous	Number	Survey	Years working in healthcare field
Years HC Privacy	Independent	Continuous	Number	Survey	Years working in healthcare privacy field
Knowledge Level	Independent	Categorical	Excellent=1 Above Average=2 Average = 3 Below Average=4 Poor=5	Survey	Self-rating on healthcare privacy knowledge level
Prior Breach Status	Independent	Categorical	No=0 Yes=1	Survey	Reported a prior breach
Profit Status	Independent	Categorical	Non-Profit= 1 For-Profit = 2	Survey	Facility of employment profit status as either non-profit or for-profit
Education Level	Independent	Categorical	High School=1 Associates=2 Bachelors=3 Masters=4 Doctoral=5	Survey	Highest level of education completed
Credential	Independent	Categorical	RHIA=1 RHIT=2 CCA=3 CCS=4 CCSP=5 CDIP=6 CHDA=7 CHPS=8 CHTS=9 CPHI=10	Survey	All AHIMA credentials held by participant
Facility Type	Control	Categorical	Acute Care=1 IHDS=2 Ambulatory = 3 Behavioral =4 Physician Practice=5 Consultant=6 Education=7 HIE=8 Home Health=9 Long Term=10 Non-Provider=11	Survey	Facility of employment type

Variable	Variable Type	Variable Classification	Measure	Source	Definition
			Other= 12 REC=13		
Gender	Control	Categorical	Male=1 Female= 2 Prefer not to disclose=3 Other=4	Survey	Gender
Age	Control	Continuous	Number	Survey	Age
Department	Control	Categorical	Executive = 1 HIM Staff = 2 IT Staff = 3 Joint=4 Other=5	Survey	Role in healthcare current position falls under
State Laws	Control	Categorical	No=0 Yes=1	Survey	Presence of additional state breach reporting laws

Bivariate Analyses of Framing Effects

A comparison of the three breach scenario questions showcased the impact that framing of a scenario has on the decision an individual privacy officer makes for breach notification determination, see Table 5 for the variables used. A chi-square test for independence was used to analyze the relationship between two categorical variables and to test the differences between these two independent groups using a significance level of 0.05 (Pallant, 2013; Hazra & Gogtay, 2016). A comparison was made of the General Breach Scenario variable against the Gain Breach Scenario variable and then compared against the Loss Breach Scenario variable. The general assumption required is that all cells in the output should have a frequency greater than or equal to five or in the case of a 2x2 table, greater than or equal to ten. If that assumption is not met, then Fisher's Exact Probability Test is utilized (Pallant, 2013). There are two separate chi-square models, but both have the following format:

$$x^2 = \sum + \frac{(O-E)^2}{E}$$ where:

x^2= chi-square obtained
$\sum$ = sum of
O= observed frequency
E = expected frequency

The research questions and hypotheses that are addressed with the bivariate chi-square tests are as follows:

RQ3: Does the framing of a scenario affect Privacy Officers' choice to report a breach of information?

H19: A breach of healthcare information scenario framed as a gain is positively associated with privacy officers classifying the breach as reportable to the Office for Civil Rights.

H20: A breach of healthcare information scenario framed as a loss is negatively associated with privacy officers classifying the breach as reportable to the Office for Civil Rights.

Software

The analysis used SPSS and Stata software through a license with the University of Central Florida. IBM SPSS Statistics 24 was used to run the descriptive analyses, correlation and chi-square tests, and multiple logistic regression models. The post regression analyses were run using Stata software.

Data Cleaning

Once the survey closed, a final review of the data was necessary to clean the data. Of the 170 responses, six respondents started the survey but did not answer a majority of questions, five stated they were not employed, and five were not their facility's Privacy Officer. Twenty of the respondents did not answer one or more of the dependent variable questions and were removed.

To ensure a clean data set, other responses were removed if they did not fully complete the survey, including three for 'Profit Status,' one for 'State Laws,' one for 'Years of healthcare privacy experience,' and six for 'Age.' This left a final of 123 survey responses which exceeded the minimum sample size required.

A few responses had issues addressed during the review of the data. There was removal of any '+' sign (for example 20+) or words for the two variables dealing with 'Years worked in healthcare.' An assumption would be that the 'Number of years worked in healthcare privacy' would be greater than or equal to the 'Number of years worked in healthcare.' Five responses did not meet this assumption. To account for this and the individual's response, there was a new variable created by dividing the two previous variables. The new variable, 'Percentage of years worked in healthcare privacy' represented the amount of their career in healthcare explicitly worked in the privacy field.

The number of responses for the options under the categories for each variable necessitated a few modifications to the original operationalization table so that they could run accurately in the model. For 'Education Level,' High School and Associates Level combined, as well as Masters and Doctoral Degree. For 'Facility Classification,' the highest proportion of respondents fell into two categories, so all the remaining were combined to Other. For 'Knowledge Level,' there were no responses for Below Average or Poor. For 'Gender,' there were no responses for Other.

The 'Credential' variable originally dedicated a number to each individual credential. However, many study participants held multiple credentials, so these were broken out. The key credentials after a review of the correlational table and demographics were RHIA/RHIT, Coding,

and CHPS credentials. These were modified to dichotomous yes/no variables, and the 'Credential' variable was changed to a dichotomous yes/no as well, signifying presence of any credential or not. As each of the individual types of credentials make up the overall 'Credential' variable as well, it was prudent to remove the 'Credential' variable in favor of the individual types of credentials to ensure overlap did not occur.

The 'Department' variable showed an interesting result after reviewing the descriptive data. Originally there were five categories, one being Other with a fill-in option. The Other option was selected numerous times with a high number of write-ins for 'Compliance.' These were parsed out with a new category of Compliance created, Executive kept as is, and the remaining categories combined to HIM/IT/Other.

Table 7: Updated Operationalization of Independent and Control Variables

Variable	Variable Type	Variable Classification	Measure	Source	Definition
% Years HC Privacy	Independent	Continuous	Number	Survey	Percent of years working in healthcare spent in privacy field
Knowledge Level	Independent	Categorical	Excellent=1 Above Average=2 Average = 3	Survey	Self-rating on healthcare privacy knowledge level
Prior Breach Status	Independent	Categorical	No=0 Yes=1	Survey	Reported a prior breach
Profit Status	Independent	Categorical	Non-Profit= 1 For-Profit = 2	Survey	Facility of employment profit status as either non-profit or for-profit
Education Level	Independent	Categorical	HS/Assoc=1 Bachelors=2 Graduate=3	Survey	Highest level of education completed
RHIA/RHIT Credential	Independent	Categorical	No=0 Yes=1	Survey	Hold a RHIA and or RHIT credential
Coding Credential	Independent	Categorical	No=0 Yes=1	Survey	Hold a coding credential
CHPS Credential	Independent	Categorical	No=0 Yes=1	Survey	Hold a CHPS credential
Facility Type	Control	Categorical	Acute Care=1 IHDS=2 Other= 3	Survey	Facility of employment type
Gender	Control	Categorical	Male=1 Female= 2 Prefer not to disclose=3	Survey	Gender
Age	Control	Continuous	Number	Survey	Age
Department	Control	Categorical	Executive = 1 HIM/IT/Other Staff = 2 Compliance=3	Survey	Role in healthcare current position falls under
State Laws	Control	Categorical	No=0 Yes=1	Survey	Presence of additional state breach reporting laws

Ethics

This study has many ethical issues to take into consideration. IRB approval was required before data collection began. The topic at hand, privacy breach reporting, was handled with the

utmost care during measurement tool creation. Privacy breach reporting has the potential to be detrimental to an organization as shown through the literature review, which could lead to a reluctance from participants. A subject matter expert reviewed the survey and provided feedback before use. To ensure the appropriateness of the questions, several individuals participated in a pilot study. Lastly, all data collected is maintained with the standards required under the UCF Institutional Review Board to ensure privacy protections.

CHAPTER 4: RESULTS

This chapter covers the findings from the analysis detailed in Chapter 3. Descriptive and bivariate statistical results are discussed. Finally the multivariate and post regression analyses used to answer the research questions from this study are detailed by method of analysis.

Descriptive Statistics

Descriptive statistics show the breakdown of invited and participating individuals (Table 8) and their demographic information (Tables 9-13). This face validity check indicated the data collected was representative of the population studied.

Table 8: Survey Requests and Participants

	Contacted	Participated	Disqualified
State with additional healthcare privacy laws	172 (36%)	48 (39%)	1
State without additional healthcare privacy laws	307 (64%)	75 (61%)	4
Total	479	123 (25%)	5

After a review of the AHIMA Engage site, 479 individuals with a Privacy designation within the United States were identified and contacted for participation. As shown in Table 8, of those who participated in the survey, 39% were in a state with additional healthcare privacy laws and 61% were in states without additional laws. This is comparable to the contacted population, where it was 36% and 64% respectively. This is representative of the AHIMA population as a whole as well, where they found 7.1% of their members were in the Privacy/Security/Compliance area and this study found about 9% of the population had a Privacy designation (479/5293) (Caviart Group, 2015). Appendix H provides details of this breakdown.

Table 9: Privacy Officer/Facility Demographic Statistics

	Mean	Median	Mode	Std. Dev.	Variance	Range	Min.	Max.
Age	53.02	54	47[a]	8.50	72.17	45	27	72
Years employed in healthcare	26.76	28	30	10.90	118.81	45	1	46
Years employed in healthcare privacy	12.55	12	15	7.21	52.02	39	1	40
Percentage of years worked in healthcare privacy	0.49	0.45	1	0.26	0.07	0.97	0.03	1
Number of breaches facility reported to OCR	34.2	12	1	57.42	3296.52	299	1	300

a. Multiple modes exist. The smallest value is shown

As shown in Table 9, the average age of respondents was 53 years old with a standard deviation of 8.5 years. The number of years they worked in healthcare was high, at close to 27 years. They also on average worked a significant amount of time in privacy, with the mean over 12 years. Many respondents worked a majority of their time in healthcare in the privacy field, with the average being close to 50%. The average number of breaches was 34 with a large range from 1-300 as expected when taking into account some respondents may have been from smaller facilities and others from large systems.

Table 10: Privacy Officer Demographics

Variable		Number	%
Age	25-34	4	3.3
	35-44	13	10.6
	45-54	49	39.8
	55-64	52	42.3
	65+	5	4.1
Gender	Female	113	91.9
	Male	10	8.1
Education	High School	2	1.6
	Associate Degree	23	18.7
	Bachelor Degree	57	46.3
	Master Degree	37	30.1
	Doctoral Degree	4	3.3
Credentials	Credentials (Y/N)	110	89.4
	RHIA	46	37.4
	RHIT	27	22
	CCS/CSS-P	9	7.3
	CHPS	18	14.6
	CHTS	1	0.8
	CPHI	1	0.8
	CDIP	1	0.8
Department	HIM Department	59	48
	IT Department	3	2.4
	Joint HIM/IT Appointment	5	4.1
	Compliance	21	17.1
	Executive Team	26	21.1
	Other	9	7.3
Knowledge Level	Excellent	47	38.2
	Above Average	60	48
	Average	16	13
% of Years worked in Healthcare Privacy	1-24	22	17.6
	25-49	51	40.8
	50-74	27	21.7
	75-99	9	7.2
	100	14	11.4

The Privacy Officer specific demographics are shown in Table 10. The ages of the Privacy Officer respondents fell in greater numbers in the 35-64 year old range, 92.7% which is consistent with numbers from an AHIMA study which found 77.3% of their members fell within the same range when taking into account their population of student members which were ineligible for this study (Caviart Group, 2015). Gender was also consistent with the study from AHIMA which showed a 91% to 9% ratio of women to men in comparison with this study which was 92% to 8% (Caviart Group, 2015).

A large percentage of respondents held at least one credential, 89.4%. The highest number had a RHIA which is a Bachelor' Degree credential, although this did not line up with the percentage of those who held that degree, 37.4% and 46.3%. This was the same for the Associate's level degree and credential, 18.7% and 22%. This was as expected since all those who qualify do not necessarily sit for the credential. The other two credentials that stood out were the coding credential category and the CHPS. Only 14.6% of those who responded held the dedicated credential that best fits with the Privacy Officer position. Also of note, the majority of the respondents had at least some level of higher education, with the majority graduating with a Bachelor's (46.3%) or Master's degree (37%).

As stated previously, when running the statistics for the 'Department' classification variable, the Other category held numerous write-ins for Compliance which necessitated the creation of another category split from Other. Compliance was the third highest department with 17.1%, behind Executive with 21.1% and HIM Department with 48%. Respondents fell into these three categories the majority of the time, accounting for over 86%. Write-in responses that

remained in the Other category were Director of Revenue Cycle, Physician Practice, Information Security, Patient Business Service, Quality, Risk Management and Corporate.

'Knowledge Level' was a self-reported variable that included five categories, Poor, Below Average, Average, Above Average, and Excellent. No respondents classified themselves as Below Average or Poor. The highest percentage self-rated as Above Average with 48%, followed by Excellent with 38.2% and finally the least at Average with 13%.

Table 11: Privacy Officer Years Employed

	In Healthcare (Number)	In Healthcare (%)	In Healthcare Privacy (Number)	In Healthcare Privacy (%)
1-9	10	8	45	36.4
10-19	18	14.6	59	48
20-29	39	31.6	14	11.4
30-39	39	31.6	5	4
40-50	17	13.7	-	-

As shown in Table 9, the survey respondents have spent an extended period of time in healthcare on average. In Table 11, this is broken down further into year categories and shows that over 63% of respondents have worked in healthcare between 20-39 years. The average time spent in healthcare privacy was 12.5 years, and Table 11 shows that the higher percentages of respondents have been in privacy less than 20 years. This is as expected as HIPAA was only created in 1996 with a 2003 effective date, which was twenty years ago. The push for Privacy Officers was not urgent until the 2009/2013 legislation as well. Table 10 also shows this, with the majority of respondents having worked 50% or less of their healthcare career in the privacy arena.

Table 12: Facility Demographics

		Number	%
Facility Classification	Acute Care Hospital	51	41.5
	Ambulatory Surgery Center	1	0.8
	Behavioral/Mental Health	7	5.7
	Clinic/Physician Practice	10	8.1
	Consulting Service	1	0.8
	Education	2	1.6
	Health Information Exchange	1	0.8
	Home Health/Hospice	1	0.8
	Integrated Healthcare Delivery System	36	29.3
	Long Term Care	4	3.3
	Non-Provider Setting (e.g., govt, vendor, assoc.)	3	2.4
	Other Provider Setting (e.g., rehab)	4	3.3
	Regional Extension Center	2	1.6
State Privacy Laws	No	75	61
	Yes	48	39
Profit Status	For-Profit	34	27.6
	Non-Profit	89	72.4

Respondents of the survey worked, by a majority, in an Acute Care Hospital, 41.5% as shown in Table 12. The second highest category was an Integrated Healthcare Delivery System with 29.3%. The other categories fell below 10% of respondents with each coming closer to 1-2%. This is somewhat in line with a study AHIMA did a few years ago where their sample came in at about 52% for Acute Care, 9% with Integrated Systems, 8% for physician clinics, and under 10% for the other categories (AHIMA, 2010). More of the respondents worked for facilities that had a Non-Profit status over For-Profit facilities (72% to 28% respectively).

Table 13: Breach Demographics

		Number	%
Prior Breach	No	39	31.7
	Yes	84	68.3
Breach Classification	Cases of Fewer than 500 patients per incident and cases of More than 500 patients per incident	18	14.6
	Fewer than 500 patients per incident ONLY	63	51.2
	More than 500 patients per incident ONLY	3	2.4
Breach Consequences	Corrective Action Plan	23	18.7
	Corrective Action Plan and OCR Fine	1	0.8
	None	60	48.8
General Scenario	Not Report	75	61
(Dependent Var. 1)	Report	48	39
Gain Scenario	Not Report	33	26.8
(Dependent Var. 2)	Report	90	73.2
Loss Scenario	Not Report	10	8.1
(Dependent Var. 3)	Report	113	91.9

Overall the study found that the majority of respondents had reported a breach, 68.3%, but not all. As shown in Table 13, For those that had reportable breaches, most respondents had only cases that affected less than 500 patients per incident, and only three respondents had exclusively cases that were major breaches that would have required media notification. Many had no consequences from the reported breach and if they did it was a Corrective Action Plan rather than fines.

The dependent variables were scenario-based; the first scenario was generic – if there is an ambiguous breach in the future, with no further information, would they report? The majority of respondents chose that they would Not Report, 61%. The second scenario, while still ambiguous, included framing of the question with a gain perspective. It involved a case with

paper records. The majority reversed in this case, with 73.2% choosing to Report. The last scenario was still ambiguous, but had a loss frame and involved a ransomware attack. In this case, an overwhelming majority chose to Report, 91.9%.

The demographics by scenario are showcased in Table 14.

Table 14: Demographics by Scenario

		General Scenario (yes)	Gain Scenario (yes)	Loss Scenario (yes)
Gender	Male	20%	80%	90%
	Female	41%	67%	92%
Education	High School	50%	100%	100%
	Associates Degree	48%	96%	100%
	Bachelor's Degree	40%	77%	91%
	Master's Degree	27%	51%	86%
	Doctoral Degree	75%	75%	100%
Credentials	No	69%	69%	100%
	Yes	35%	74%	91%
Department	Executive	38%	73%	96%
	HIM/IT/Joint	38%	75%	93%
	Staff/Other Compliance	43%	57%	81%
Knowledge	Excellent	38%	62%	87%
	Above Average	40%	80%	95%
	Average	38%	81%	94%
Age	Mean	54	53	53
PercYrsWrkd	Mean	49%	47%	48%

As showcased in Table 14, there were differences in the demographics of Privacy Officers by scenario. Females reported 'Yes, they would report' to a general scenario at a higher percentage, 41% compared to 20% of males. However, that switches with a gain scenario, where 80% of males reported 'Yes' as opposed to 67% of females. For the loss scenario, the percentages were fairly similar, 90% (males) and 92% (females). Differences are shown among education levels and reporting, the lowest percentage was for Master's Degree holding Privacy

Officers in a general scenario at 27% and a highest percentage at High School education level Privacy Officers in both a gain and loss scenario as well as Doctoral Degree Privacy Officers in a loss scenario, all at 100% reporting rates.

There were large differences among credential holders in a general and loss scenario, 35% and 91% respectively. Department level showed large differences among scenarios however, these percentages were steady among department levels, with the lowest percentages reporting 'Yes' for the general scenario and the highest percentages reporting 'Yes' for the loss scenario. This trend was evident with the knowledge level as well, even among the levels ranging from lowest with the general scenario and highest with the loss scenario. The mean for Age was even across all scenarios as well as for percentage of years worked in healthcare.

Bivariate Analysis of Breach Reporting

Chi-square explores the relationship between two categorical variables as it compares the frequencies of cases in each category against expected values to determine if there is an association (Pallant, 2013). A comparison of the calculated chi-square statistic with the chi-square distribution determined the probability of the test results. The test is suitable for use as there are independent observations with mutually exclusive categories (Boslaugh, 2013). The independent and control variables were individually tested with each of the breach scenarios (dependent variables) with a significance level of 0.05.

For the first dependent variable, there was a significant result between the General Breach Scenario and Credential. The counts are provided in Table 15.

Table 15: Chi-Square - General & Credential Counts

			Credential Y/N Recode		Total
			No	Yes	
General Breach Scenario	Not Report	Count	4 (3.3%)	71 (57.7%)	75 (61%)
	Report	Count	9 (7.3%)	39 (31.7%	48 (39%)
Total		Count	13 (10.6%)	110 (89.4%)	123 (100%)

Note: χ^2 = 4.25, df = 1. Parentheses indicate column percentages

*p=0.039

A Chi-square test for independence (with Yates Continuity Correction) indicated a significant association between the General Breach Scenario and Credential Status x^2 (1, n = 123) = 4.25, p = .039, phi = -.21 (small to medium effect size).

The following variables when tested with the General Breach Scenario were not significant at the 0.05 level:

1. Gender x^2 (1, n = 123) = .900, p = .343, phi = 0.116
2. Education x^2 (2, n = 123) = 1.81, p = .404, cramer's v = .121
3. RHIA/RHIT x^2 (1, n = 123) = .560, p = .454, phi = -0.084
4. CHPS x^2 (1, n = 123) = 3.397 p = .065, phi = -0.190
5. Coding x^2 (1, n = 123) = 2.040 p = .153, phi = -0.161
6. Department x^2 (2, n = 123) = .157, p = .924, cramer's v = .036
7. State x^2 (1, n = 123) = .218, p = .641, phi = -.059
8. Facility Class x^2 (2, n = 123) = 1.44, p = .486, cramer's v = 0.108.
9. Profit Status x^2 (1, n = 123) = .101, p = .751, phi = -.047
10. Knowledge Level x^2 (2, n = 123) = .050, p = .975, cramer's v = 0.020
11. Prior Breach x^2 (1, n = 123) = 3.514, p = .061, phi = .187

For the second dependent variable, there was a significant result between the Gain Breach Scenario and Education Level. The counts are provided in Table 16.

Table 16: Chi-Square - Gain & Education Counts

			Education Level			
			High School/Some College	Bachelor's Degree	Graduate Degree	Total
Gain Breach Scenario	Not Report	Count	1 (0.8%)	13 (10.6%)	19 (15.4%)	33 (26.8%)
	Report	Count	24 (19.5%)	44 (35.8%)	22 (17.9%)	90 (73.2%)
Total		Count	25 (20.3%)	57 (46.3%)	41 (33.3%)	123 (100%)

Note: χ^2 = 15.06, df = 2. Parentheses indicate column percentages
p= 0.001

A Chi-square test for independence indicated a significant association between Gain Breach Scenario and education level x^2 (2, n = 123) = 15.06, p = .001, cramer's v = 0.350 (medium effect size)

There was another significant result between the Gain Breach Scenario and the Coding Credential. The counts are provided in Table 17.

Table 17: Chi-Square - Gain & Coding Counts

			Coding Credential		
			No	Yes	Total
Gain Breach Scenario	Not Report	Count	27 (22%)	6 (4.9%)	33 (26.8%)
	Report	Count	27 (70.7%)	3 (2.4%)	90 (73.2%)
Total		Count	114 (92.7%)	9 (7.3%)	123 (100%)

Note: χ^2 = 5.813, df = 1. Parentheses indicate column percentages
p=0.016

A Chi-square test for independence indicated a significant association between Gain Breach Scenario and coding credential x^2 (1, n = 123) = 5.813, p = .016, phi = -0.253 (small effect size).

The following variables when tested with the Gain Breach Scenario were not significant at 0.05 level:

1. Gender x^2 (1, n = 123) = .019, p = .892, phi = -.046
2. Credentials x^2 (1, n = 123) = .000, p = .994, phi = .031
3. RHIA/RHIT x^2 (1, n = 123) = .747, p = .388, phi = .097
4. CHPS x^2 (1, n = 123) = 2.365 p = .124, phi = -0.165
5. Department x^2 (2, n = 123) = 3.519, p = .172, cramer's v = .169
6. State x^2 (1, n = 123) = 1.196, p = .274, phi = -.117
7. Facility Class x^2 (2, n = 123) = 2.951, p = .229, cramer's v = 0.155
8. Profit Status x^2 (1, n = 123) = .000, p = 1.00, phi = .005
9. Knowledge Level x^2 (2, n = 123) = 5.106, p = .078, cramer's v = 0.204
10. Prior Breach x^2 (1, n = 123) = .178, p = .674, phi = -.058

There were no significant associations at the 0.05 level between any of the variables and the Loss Breach Scenario:

1. Gender x^2 (1, n = 123) = .000, p = 1.000, phi = .020
2. Education x^2 (2, n = 123) = 3.151, p = .207, cramer's v = .160
3. Credentials x^2 (1, n = 123) = .357, p = .550, phi = -.102
4. CHPS x^2 (1, n = 123) = .936 p = .333, phi = -0.129
5. Department x^2 (2, n = 123) = 4.235, p = .120, cramer's v = .186
6. State x^2 (1, n = 123) = .163, p = .686, phi = -.067
7. Facility Class x^2 (2, n = 123) = .010, p = .995, cramer's v = .009
8. Knowledge Level x^2 (2, n = 123) = 2.215, p = .330, cramer's v = 0.134
9. Prior Breach x^2 (1, n = 123) = .226, p = .634, phi = -.075
10. Profit Status x^2 (1, n = 123) = .038, p = .845, phi = .051

Research Question and Hypothesis Testing

This study aimed to address the problem surrounding the unclear nature of breach reporting by applying Prospect Theory to better understand how Privacy Officer's make the reporting determinations. The survey provided three scenarios, a General Breach Scenario, a Gain Breach Scenario, and a Loss Breach Scenario. The outcomes of these scenarios were the three dependent variables identified for the logistic regression models. These three models address research question one with hypotheses 1-15 and research question two with hypotheses

16-18. Among these there were six hypotheses addressed by three separate models (one for each dependent variable).

The dependent variables were then compared with chi-square analyses to identify any differences among them, which addresses research question three and hypotheses 19 and 20. The next section details the results of the testing. The first set of results addresses the three models which answer research questions one and two followed by the results of the chi-square analysis that answers research question three.

General Breach Reporting Analysis

The following section will review the tests for assumptions including Tolerance and VIF tests, independent variable correlation analyses, model goodness of fit tests, and the multivariate logistic regression model results for the General Breach Reporting to answer the following research questions and hypotheses:

RQ1: Does the Privacy Officers' reference point based on knowledge levels affect their choice to report a breach of patient information?

H1: Higher percentage of years employed in the healthcare field is positively associated with reporting future indefinable breaches of healthcare information in a general scenario.

H4: Lower level of self-reported knowledge in healthcare privacy is negatively associated with reporting future indefinable breaches of healthcare information in a general scenario.

H7: Higher levels of education are positively associated with reporting future indefinable breaches of healthcare information in a general scenario.

H10: Attainment of a Certified Healthcare Privacy and Security credential is positively associated with reporting future indefinable breaches of healthcare information in a general scenario.

H13: Attainment of a Registered Health Information Administrator or Technician credential is positively associated with reporting future indefinable breaches of healthcare information in a general scenario.

RQ2: Does the Privacy Officers' reference points based on past reporting affect their choice to report a breach of patient information?

H16: Prior reporting of a breach of healthcare information to the Office for Civil Rights is positively associated with reporting future indefinable breaches of healthcare information in a general scenario.

Tolerance/VIF Tests

The Tolerance/VIF test is used to test for the limited assumptions of logistic regression. The Tolerance/VIF test for lack of multicollinearity is shown in Table 18.

Table 18: Tolerance/VIF

	General Scenario	
	Tolerance	VIF
Age	0.794	1.259
Gender	0.927	1.079
Education	0.756	1.324
RHIA and RHIT Credential	0.836	1.196
CHPS Credential	0.840	1.190
Coding Credential	0.854	1.171
Department	0.801	1.248
State Privacy Laws	0.839	1.191
Facility Classification	0.861	1.161
Profit Status	0.798	1.254
% of years worked in healthcare	0.854	1.171
Knowledge Level	0.751	1.331
Prior Breach Status	0.672	1.489

If Tolerance levels are below 0.10 or if VIF values above 10, this would indicate a high correlation between independent variables. As shown in Table 17, all variables had scores outside of these ranges, so the test shows a lack of multicollinearity to meet the assumption.

Correlation

An additional method to test for lack of multicollinearity is through correlation analysis of the independent variables in the model. Table 19 shows the correlations between all independent variables. 'Breach Outcome' and 'Breach Classification' had a very high correlation with 'Prior Breach Status' so they were not included in the final model. 'Years Employed in Healthcare' and 'Years Employed in Healthcare Privacy' were removed from the models as they both had high correlations with other variables and only the 'Percentage of

Years' was included. All other correlations between two independent variables or among control variables were small which demonstrated a lack of multicollinearity.

Table 19: Correlation of Variables

	Gender	Education Level	Credentials - General	RHIA/RHIT Cred.	CHPS Cred.	Coding Cred.	Dept.	State Privacy Laws	Facility Class	Profit Status	Yrs Emplyd Healthcare	Yrs Emplyd Healthcare Privacy	% Yrs Emplyd HC Privacy	Knowlege Level	Prior Breach Status	Breach Outcome	Breach Class.	General Breach Scenario	Gain Breach Scenario	Loss Breach Scenario
Age	0.040	-.202*	-0.065	-0.076	-0.148	0.040	-0.093	-0.057	-0.022	0.045	.591**	.322**	-0.133	-0.074	.219*	-.222*	-.252**	0.078	-0.007	0.092
Gender		-0.070	-0.006	0.057	-0.045	0.084	-0.164	-0.006	0.028	-0.082	0.049	-0.027	-0.062	0.155	-0.011	-0.058	-0.007	0.116	-0.046	0.020
Education Level			-0.085	-0.172	0.149	-0.051	.250**	-0.006	-0.014	0.015	-.236**	0.000	0.166	-.235**	.196*	-.221*	-0.176	-0.121	-.349**	-0.153
Credentials - General				.415**	0.142	0.097	-0.066	0.058	-.177*	-0.024	0.032	0.078	0.051	-0.090	-0.064	0.053	0.029	-.213*	0.031	-0.102
RHIA/RHIT					.202*	0.169	-0.055	0.017	-.201*	-0.007	0.067	0.010	-0.037	0.084	-0.102	0.028	0.066	-0.084	0.097	-0.065
CHPS Credential						-0.028	-0.010	-0.048	-0.022	-0.050	-0.038	-0.006	0.010	-.222*	0.084	-0.103	0.003	-.190*	-0.165	-0.129
Coding Credential							-0.032	.287**	-0.071	-0.034	0.126	-0.017	-0.121	0.106	-0.010	-0.016	-0.010	-0.161	-.253**	-.259**
Department								-0.082	-0.152	-0.166	-0.006	-0.081	-0.011	0.015	.295**	-.312**	-.181*	0.026	-0.099	-0.164
State Privacy Laws									0.017	0.139	0.090	0.031	-0.086	-0.097	0.044	-0.015	-0.109	-0.059	-0.117	-0.067
Facility										0.025	-0.064	0.064	0.113	-.230*	-0.121	0.094	0.079	0.097	-0.089	-0.008
Profit Status											-0.061	-0.141	-0.089	-0.066	-.321**	.306**	.199*	-0.047	0.005	0.051
Yrs Emplyd												.390**	-.366**	-0.122	.288**	-.281**	-.262**	0.119	-0.064	-0.028
Yrs Emplyd Healthcare Privacy													.620**	-.381**	0.066	-0.072	-0.071	0.054	-0.098	-0.118
% Yrs Emplyd HC Privacy														-.212*	-0.139	0.120	0.128	-0.013	-0.099	-0.085
Knowlege Level															-0.100	0.120	0.119	0.002	.183*	0.110
Prior Breach Status																-.906**	-.866**	.187*	-0.058	-0.075
Breach Outcome																	.811**	-.186*	0.091	0.111
Breach Classification																		-.194*	0.012	0.015

*. Correlation is significant at the 0.05 level (2-tailed).

**. Correlation is significant at the 0.01 level (2-tailed).

c. Cannot be computed because at least one of the variables is constant.

Predicting Factors of a General Breach Scenario

A multivariate logistic regression model was performed to examine the impact that experience and reference points have on the likelihood that survey respondents would report a breach to the Office for Civil Rights in a general scenario (Pallant, 2013). Results show the omnibus test of the model coefficients, model fit, and the predicting factors mentioned above for the General Breach Scenario. The General Breach scenario had a bivariate outcome of Yes or No.

To determine the goodness of fit of the multivariate logistic regression model, goodness of fit tests were performed. One of these is an omnibus test of coefficients which tests if the model as a whole is better than using a null model with no coefficients (Boslaugh, 2013). Hosmer-Lemeshow Goodness of Fit Test provides the chi-square statistic for this purpose. For this model the test indicated the chi-square = 4.957, df = 8, and p=0.762. The significance level is above 0.05 indicates support for the model.

Table 20 shows the results of the multivariate logistic regression analysis.

Table 20: Logistic Regression - General Scenario

				95% C.I.for EXP(B)			Hypothesis Test		
		B	Std. Error	EXP(B)	Lower	Upper	Wald Chi-Square	df	Sig.
	Intercept	-1.174	2.122	0.309			0.306	1	0.58
	Age	-0.01	0.028	0.99	0.937	1.046	0.135	1	0.713
Gender	Male	Reference	-	-	-	-	-	-	-
	Female	1.235	0.892	3.437	0.599	19.733	1.917	1	0.166
Education Level	High School/Associate Degree	Reference	-	-	-	-	-	-	-
	Bachelor's Degree	-0.193	0.598	0.825	0.255	2.664	0.104	1	0.747
	Graduate Education	-1.042	0.724	0.353	0.085	1.456	2.076	1	0.15
Credentials	RHIA/RHIT Credential (Y)	-0.017	0.441	0.983	0.414	2.332	0.002	1	0.969
	CHPS Credential (Y)	-1.94	0.819	0.144	0.029	0.716	5.605	1	0.018*
	Coding Credential (Y)	-1.798	1.177	0.166	0.016	1.663	2.334	1	0.127
Department	Executive	Reference	-	-	-	-	-	-	-
	HIM/IT/Joint/Other	-0.483	0.613	0.617	0.186	2.05	0.621	1	0.431
	Compliance	0.267	0.759	1.306	0.295	5.785	0.123	1	0.725
	State privacy laws (Y)	-0.198	0.46	0.821	0.333	2.021	0.185	1	0.667
Facility Classification	Acute Care Hospital	Reference	-	-	-	-	-	-	-
	Integrated Healthcare Delivery System	0.182	0.589	1.199	0.378	3.802	0.095	1	0.758
	Other	0.611	0.569	1.842	0.604	5.612	1.154	1	0.283
Profit Status	Not for Profit	Reference	-	-	-	-	-	-	-
	For Profit	0.259	0.558	1.296	0.434	3.872	0.215	1	0.643
	% of years worked in healthcare	0.042	0.88	1.043	0.186	5.855	0.002	1	0.962
Knowledge Level	Excellent	Reference	-	-	-	-	-	-	-
	Above Average	-0.3	0.486	0.741	0.286	1.921	0.381	1	0.537
	Average	-0.081	0.773	0.922	0.203	4.198	0.011	1	0.917
	Prior Breach (Y)	1.487	0.576	4.422	1.431	13.663	6.669	1	0.010*

N=123

*Indicates statistical significance at $p \leq .05$

Cox & Snell R Square = 0.173

Nagelkerke R Square = 0.235

Table 20 presents results from the logistic regression model, which predicts the reporting of a General Breach Scenario. The model contained five independent variables (Education Level, Credentials, Percentage of years worked in healthcare, Knowledge Level, and Prior Breach Status). For this model, the CHPS credential and Prior Breach Status were significantly associated with reporting a breach. The CHPS credential was significant at p=0.018 with an odds ratio of 0.144 indicating that an individual with a CHPS credential, with limited information, is 0.144 times less likely than someone without a CHPS credential reporting a general breach to OCR. Prior Breach Status was statistically significant as well at p=0.010 with an odds ratio of 4.422 indicating that a respondent who had reported a prior breach is 4.422 times more likely to report a general breach, with limited information, to OCR than a respondent who had not reported a prior breach. Due to the high odds ratio of the Prior Breach variable, a univariate model was attempted to understand the impact that particular variable had on the model. Once the data were split between two new data sets the numbers were not sufficient to run the logistic regression models. The Cox & Snell R Square and Nagelkerke R Square indicate the amount of variation in the dependent variable explained by the model (Pallant, 2013). The variation determined by the model is between 17.3% and 23.5%.

Gain Breach Reporting Analysis

The following section will review the tests for assumptions including Tolerance and VIF tests, independent variable correlation analyses, model goodness of fit tests, and the multivariate logistic regression model results for the Gain Breach Reporting to answer the following research questions and hypotheses:

RQ1: Does the Privacy Officers' reference point based on knowledge levels affect their choice to report a breach of patient information?

H2: Higher percentage of years employed in the healthcare field is positively associated with reporting future indefinable breaches of healthcare information in a gain scenario.

H5: Lower level of self-reported knowledge in healthcare privacy is negatively associated with reporting future indefinable breaches of healthcare information in a gain scenario.

H8: Higher levels of education are positively associated with reporting future indefinable breaches of healthcare information in a gain scenario.

H11: Attainment of a Certified Healthcare Privacy and Security credential is positively associated with reporting future indefinable breaches of healthcare information in a gain scenario.

H14: Attainment of a Registered Health Information Administrator or Technician credential is positively associated with reporting future indefinable breaches of healthcare information in a gain scenario.

RQ2: Does the Privacy Officers' reference points based on past reporting affect their choice to report a breach of patient information?

H17: Prior reporting of a breach of healthcare information to the Office for Civil Rights is positively associated with reporting future indefinable breaches of healthcare information in a gain scenario.

Tolerance/VIF Tests

The Tolerance/VIF test is used to test for the limited assumptions of logistic regression. The Tolerance/VIF test for lack of multicollinearity is shown in Table 21.

Table 21: Tolerance/VIF

	Gain Scenario	
	Tolerance	VIF
Age	0.794	1.259
Gender	0.927	1.079
Education	0.756	1.324
RHIA and RHIT Credential	0.836	1.196
CHPS Credential	0.840	1.190
Coding Credential	0.854	1.171
Department	0.801	1.248
State Privacy Laws	0.839	1.191
Facility Classification	0.861	1.161
Profit Status	0.798	1.254
% of years worked in healthcare	0.854	1.171
Knowledge Level	0.751	1.331
Prior Breach Status	0.672	1.489

As shown in Table 21, all variables had Tolerance/VIF scores outside of the high correlation ranges (Tolerance >0.10 or VIF <10), therefore there is a low risk of multicollinearity in the multivariate logistic regression model predicting the reporting of a breach in a gain scenario.

Correlation

An additional method to test for a lack of multicollinearity is through correlation analysis of the independent variables in the model. Table 19 shows the correlations between all independent variables. 'Breach Outcome' and 'Breach Classification' had a very high

correlation with ‘Prior Breach Status’ so they were not included in the final model. ‘Years Employed in Healthcare’ and ‘Years Employed in Healthcare Privacy’ were removed from the models as they both had high correlations with other variables and only the ‘Percentage of Years’ was included . All other correlations between two independent variables or among control variables were small which demonstrated a lack of multicollinearity.

Predicting Factors of a Gain Breach Scenario

A multivariate logistic regression model examined the impact that experience and reference points have on the likelihood that survey respondents would report a breach to the Office for Civil Rights in a gain scenario (Pallant, 2013). Results show the omnibus test of the model coefficients, model fit, and the predicting factors mentioned above for the General Breach Scenario. The Gain Breach Scenario had a bivariate outcome of Yes or No.

To determine the goodness of fit of the multivariate logistic regression model, goodness of fit tests were performed. For this model the test indicated the chi-square = 5.530, df = 8, and p=0.700. The significance level is above 0.05 indicating support for the model.

Table 22 shows the results of the multivariate analysis.

Table 22: Logistic Regression - Gain Scenario

					95% C.I.for EXP(B)		Hypothesis Test		
		B	Std. Error	EXP(B)	Lower	Upper	Wald Chi-Square	df	Sig.
	Intercept	7.662	2.784	2126.323			7.576	1	0.006
	Age	-0.031	0.032	0.969	0.911	1.031	0.976	1	0.323
Gender	Male	Reference	-	-	-	-	-	-	-
	Female	-1.100	0.969	0.333	0.050	2.223	1.290	1	0.256
Education Level	High School/Associate's Degree	Reference	-	-	-	-	-	-	-
	Bachelor's Degree	-3.318	1.490	0.036	0.002	0.672	4.958	1	0.026*
	Graduate Education	-4.317	1.568	0.013	0.001	0.288	7.585	1	0.006*
Credentials	RHIA/RHIT Credential (Y)	0.693	0.569	1.999	0.655	6.100	1.480	1	0.224
	CHPS Credential (Y)	-1.347	0.697	0.260	0.066	1.019	3.736	1	0.053
	Coding Credential (Y)	-3.667	1.270	0.026	0.002	0.308	8.337	1	0.004*
Department	Executive	Reference	-	-	-	-	-	-	-
	HIM/IT/Joint/Other	-0.723	0.754	0.485	0.111	2.127	0.920	1	0.338
	Compliance	-0.902	0.883	0.406	0.072	2.291	1.043	1	0.307
	State privacy laws (Y)	-0.331	0.555	0.718	0.242	2.131	0.356	1	0.551
Facility Classification	Acute Care Hospital	Reference	-	-	-	-	-	-	-
	Integrated Healthcare Delivery System	0.004	0.703	1.004	0.253	3.981	0.000	1	0.996
Profit Status	Not for Profit	Reference	-	-	-	-	-	-	-
	For Profit	0.312	0.715	1.367	0.336	5.552	0.191	1	0.662
	% of years worked in healthcare	-0.613	0.992	0.542	0.077	3.791	0.381	1	0.537
Knowledge Level	Excellent	Reference	-	-	-	-	-	-	-
	Above Average	0.525	0.542	1.691	0.585	4.889	0.940	1	0.332
	Average	0.981	1.110	2.667	0.303	23.477	0.781	1	0.377
	Prior Breach (Y)	0.650	0.738	1.915	0.451	8.130	0.776	1	0.378

N=123

*Indicates statistical significance at $p \leq .05$

Cox & Snell R Square = 0.272

Nagelkerke R Square = .395

The model contained five independent variables (Education Level, Credentials, Percentage of years worked in healthcare, Knowledge Level, and Prior Breach Status). For this model, three of the independent variables were statistically significant. The Bachelor's Degree was significant at p=0.026 with an odds ratio of 0.036 indicating that someone with a Bachelor's Degree reporting a breach, with limited information but framed from a Gain point of view, to OCR is 0.036 times less likely than someone with a High School or Associate's Degree. Graduate Education was statistically significant as well at p=0.006 with an odds ratio of 0.013 indicating that a respondent who with a Graduate Education is 0.013 times less likely to report a breach, with limited information but framed from a Gain point of view, to OCR. The third independent variable that was statistically significant was Coding Credential at p=0.004 with an odds ratio of 0.026 indicating that a respondent with a Coding Credential reporting a breach, with limited information but framed from a Gain point of view, to OCR is 0.026 times less likely than a respondent without a Coding Credential. The Cox & Snell R Square and Nagelkerke R Square indicate the amount of variation in the dependent variable explained by the model (Pallant, 2013). The variation determined by the model is between 27.2% and 39.5%.

Loss Breach Reporting Analysis

The following section will review the tests for assumptions including Tolerance and VIF tests, independent variable correlation analyses, model goodness of fit tests, and the multivariate logistic regression model results for the Loss Breach Reporting to answer the following research questions and hypotheses:

RQ1: Does the Privacy Officers' reference point based on knowledge levels affect their choice to report a breach of patient information?

H3: Higher percentage of years employed in the healthcare field is positively associated with reporting future indefinable breaches of healthcare information in a loss scenario.

H6: Lower level of self-reported knowledge in healthcare privacy is negatively associated with reporting future indefinable breaches of healthcare information in a loss scenario.

H9: Higher levels of education are positively associated with reporting future indefinable breaches of healthcare information in a loss scenario.

H12: Attainment of a Certified Healthcare Privacy and Security credential is positively associated with reporting future indefinable breaches of healthcare information in a loss scenario.

H15: Attainment of a Registered Health Information Administrator or Technician credential is positively associated with reporting future indefinable breaches of healthcare information in a loss scenario.

RQ2: Does the Privacy Officers' reference points based on past reporting affect their choice to report a breach of patient information?

H18: Prior reporting of a breach of healthcare information to the Office for Civil Rights is positively associated with reporting future indefinable breaches of healthcare information in a loss scenario.

Tolerance/VIF

The Tolerance/VIF test is used to test for the limited assumptions of logistic regression. The Tolerance/VIF test for lack of multicollinearity is shown in Table 23.

Table 23: Tolerance/VIF

	Loss Scenario	
	Tolerance	VIF
Age	0.794	1.259
Gender	0.927	1.079
Education	0.756	1.324
RHIA and RHIT Credential	0.836	1.196
CHPS Credential	0.840	1.190
Coding Credential	0.854	1.171
Department	0.801	1.248
State Privacy Laws	0.839	1.191
Facility Classification	0.861	1.161
Profit Status	0.798	1.254
% of years worked in healthcare	0.854	1.171
Knowledge Level	0.751	1.331
Prior Breach Status	0.672	1.489

As shown in Table 23, all variables had scores outside of the high correlation ranges (Tolerance >0.10 or VIF <10), so the test shows a lack of multicollinearity to meet the assumption.

Correlation

Table 19 shows the correlations between all variables which tests for the lack of multicollinearity. 'Breach Outcome' and 'Breach Classification' had a very high correlation with 'Prior Breach Status' so they were not included in the final model. 'Years Employed in Healthcare' and 'Years Employed in Healthcare Privacy' were removed from the models as they both had high correlations with other variables and only the 'Percentage of Years' was included . All other correlations between two independent variables or among control variables were small which demonstrated a lack of multicollinearity.

While the study met the overall assumptions for logistic regression including a lack of multicollinearity, the data set was homogenous in the outcome as indicated in Figure 9.

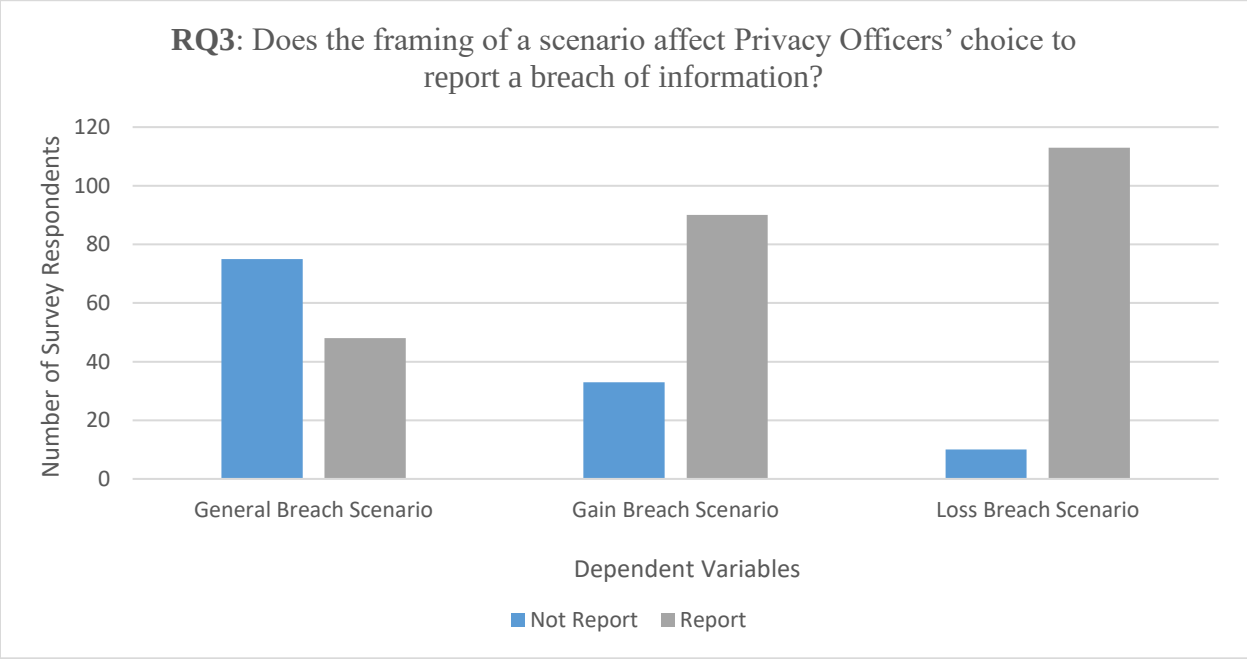

Figure 9: Scenario Framing Distribution

Figure 9 shows that of the 123 respondents, 91.9% (113) chose Yes they would report the breach while 8.1% (10) respondents chose No they would not report. The Loss Breach Scenario in Figure 9 indicated that there was no need to run a model of predicting factors.

Post Regression Analysis

After running the logistic regression models, predicted probabilities were calculated using marginal standardization. In this technique, the estimate of breach reporting was "proportionally adjusted according to a weight for each level of the confounding factors" (Muller and MacLehose, 2014). These predicted probabilities range from 0% to 100% (Muller and MacLehose, 2014). Table 24 shows the results of the predicted probabilities.

Table 24: Predicted Probabilities of Multivariate Logistic Regression

		General	Gain
Gender	Male (ref)	0.202	0.875
	Female	0.396	0.709
Education Level	High School/Associate Degree (ref)	0.482	0.982
	Bachelor's Degree	0.417	0.716**
	Graduate Education	0.272	0.562**
RHIA Credential	No (ref)	0.371	0.675
	Yes	0.396	0.790
CHPS Credential	No (ref)	0.427	0.760
	Yes	0.127**	0.575**
Coding Credential	No (ref)	0.401	0.767
	Yes	0.130	0.261**
Department	Executive (ref)	0.441	0.813
	HIM/IT/Joint/Other	0.340	0.715
	Compliance	0.468	0.666
State Privacy Laws	No (ref)	0.404	0.750
	Yes	0.339	0.685
Facility Classification	Acute Care Hospital (ref)	0.329	0.742
	Integrated Healthcare Delivery System	0.370	0.763
	Other	0.463	0.652
Profit Status	Not for Profit (ref)	0.366	0.713
	For Profit	0.421	0.759
Knowledge Level	Excellent (ref)	0.405	0.657
	Above Average	0.353	0.765
	Average	0.413	0.860
Prior Breach Status	No (ref)	0.209	0.666
	Yes	0.472**	0.751

Significance denotes differences from reference category
* p<0.1 ; ** p<0.05 ; *** p<0.001

Under the General Breach Scenario, holding everything else constant, the CHPS Credential variable and the Prior Breach Status variable were significant at the 0.05 alpha level. Privacy Officers that hold the CHPS Credential are less likely to report a breach under a general scenario (predicted probability of 12.7% for those with the CHPS Credential, versus 42.7% for

those who do not have the credential). Privacy Officers that have previously reported a prior breach are more likely to report a breach under a general scenario (predicted probability of 47.2% with a prior breach, versus 20.9% with no prior reported breaches).

Under the Gain Breach Scenario, holding everything else constant, Bachelor's Degree and Graduate Education as well as the CHPS Credential and the Coding Credential were significant at the 0.05 level. Privacy Officers that have a Bachelors or Graduate Education are less likely to report a breach under a gain scenario (predicted probability of 56.2% for those with a graduate education and 71.6% for those with a bachelor's degree, versus 98.2% for those with a high school diploma or an associate's degree). Privacy Officers that hold the CHPS Credential are less likely to report a breach under a gain scenario (predicted probability of 57.5% for those with the CHPS Credential, versus 76% for those who do not have the credential). Privacy Officers that hold a Coding Credential are less likely to report a breach under a gain scenario (predicted probability of 26.1% for those with a Coding Credential, versus 76.7% for those who do not have the credential).

Bivariate Analysis of Framing Effects

The final research question examines the impact framing has on the choice Privacy Officers make to report a breach to OCR. The three categorical dependent variables are compared for this analysis to determine statistical differences in the choices the respondents made. The analysis between the General Breach Scenario variable and the Gain Breach Scenario variable are shown in Table 25.

Table 25: Chi-Square - General & Gain Counts

			Gain Scenario		Total
			No	Yes	
General Breach Scenario	Not Report	Count	27 (22%)	48 (39%)	75 (61%)
	Report	Count	6 (4.9%)	42 (34.1)	48 (39%)
Total		Count	33 (26.8%)	90 (73.2%)	123 (100%)

Note: χ^2 = 7.08, df = 1. Parentheses indicate column percentages
p=0.008

The chi-square test for independence (with Yates Continuity Correction) as shown in Table 24 indicated a significant association between the General Breach Scenario and the Gain Breach Scenario x^2 (1, n = 123) = 7.080, p = .008, phi = .259 (small effect size). Therefore the chi-square analysis shows the proportion of respondents reporting in a general scenario is statistically different from the proportion of respondents reporting in a gain scenario.

The analysis between the Gain Breach Scenario variable and the Loss Breach Scenario variable is shown in Table 26.

Table 26: Chi-Square - Gain & Loss Counts

			Loss Breach Scenario		
			Not Report	Report	Total
Gain Breach Scenario	Not Report	Count	9 (7.3%)	24 (19.5%)	33 (26.8%)
	Report	Count	1 (0.8%)	89 (72.4%)	90 (73.2%)
Total		Count	10 (8.1%)	113 (91.9%)	123 (100%)

Note: χ^2 = 18.762, df = 1. Parentheses indicate column percentages
p= 0.000

A Chi-square test for independence (with Fisher's Exact Test) indicated a significant association between Gain Breach Scenario and Loss Breach Scenario x^2 (1, n = 123) = 18.762, p = .000, phi = .424 (medium effect size). Therefore the chi-square analysis shows the proportion

of respondents reporting in a gain scenario is statistically different from the proportion of respondents reporting in a loss scenario.

Review of Open-Ended Comments

The final question of the survey was an open-ended question which cited a recent journal published by AHIMA and asked for feedback from participants. The question was as follows: "The April 2017 cover story for the Journal of AHIMA was titled "Is HIPAA Outdated?" What are your thoughts regarding the HIPAA legislation in terms of breach notification and its ability to adapt? Please add any additional comments regarding breach notification that you feel would be useful to this study." Open coding of the responses was performed to identify key themes (Corbin & Strauss, 2014). These themes and example comments are located in Table 27.

Table 27: Open-Ended Comments

Themes	Quotes
Need for Clarification/Guidance/More Information	"Additional clarity is needed around determining if a breach is reportable." "I feel we need more detailed guidelines as far as exact procedures/practices on how to protect PHI…"
Current Law Descriptions – Negative	"I think it is outdated and the requirements are getting more cumbersome and draconian to implement and maintain compliance." "The HIPAA policy could definitely use an update. Technology has significantly advanced since the law was enacted."
Current Law Descriptions – Positive	"I believe there were improvements with Omnibus and breach notification which made assessment more objective and consistent (ie., four factor analysis), and provided a method for good documentation about how privacy officers reached their conclusions…" "I do not think HIPAA is outdated, since its provisions remain relevant."
Consideration of new security issues	"I feel that phishing and cyberattacks are not fully able to be vetted through the current four-step process very well…" "Cumbersome but necessary - cyber attacks are concerning - government mandates for quality programs take away money that could be spent to help assess / prevent risks related to breaches - it is a catch 22"
Electronic/Technological Updates	"HIPAA was created in the VCR era. We have a lot more technology, such as smart phones, social media that brings an whole new scope of HIPAA into play" "Unfortunately, current legislation has not caught up to technological advances and risks"

CHAPTER 5: DISCUSSION

This chapter summarizes the findings from the hypotheses test and their impact on the research questions, details the theoretical contributions as well as the practical contributions, discusses the implications of the findings for Public Affairs, points out the limitations of the study, explores areas of future research, and provides a conclusion for the study.

Summary of Hypotheses

Reporting a breach of patient information is not inherently good or bad. Depending on the circumstances and the individual's viewpoint it could be one or both. The key here is the scenarios are dealing with ambiguous breaches, they could or could not be harmful to the patient. There is an unknown element.

Research question one explored the effects a respondent's reference point based on knowledge levels had on the choice to report a breach of patient information. The results of the hypotheses testing for research question one are located in Table 28.

Table 28: Hypothesis Testing RQ 1

	Alternative Hypothesis	Outcome
H1	Higher percentage of years employed in the healthcare field is positively associated with reporting future indefinable breaches of healthcare information in a general scenario.	Fail to reject null hypothesis
H2	Higher percentage of years employed in the healthcare field is positively associated with reporting future indefinable breaches of healthcare information in a gain scenario.	Fail to reject null hypothesis
H3	Higher percentage of years employed in the healthcare field is positively associated with reporting future indefinable breaches of healthcare information in a loss scenario.	Fail to reject null hypothesis

	Alternative Hypothesis	Outcome
H4	Lower level of self-reported knowledge in healthcare privacy is negatively associated with reporting future indefinable breaches of healthcare information in a general scenario.	Fail to reject null hypothesis
H5	Lower level of self-reported knowledge in healthcare privacy is negatively associated with reporting future indefinable breaches of healthcare information in a gain scenario.	Fail to reject null hypothesis
H6	Lower level of self-reported knowledge in healthcare privacy is negatively associated with reporting future indefinable breaches of healthcare information in a loss scenario.	Fail to reject null hypothesis
H7	Higher levels of education are positively associated with reporting future indefinable breaches of healthcare information in a general scenario.	Fail to reject null hypothesis
H8	Higher levels of education are positively associated with reporting future indefinable breaches of healthcare information in a gain scenario.	Fail to reject null hypothesis
H9	Higher levels of education are positively associated with reporting future indefinable breaches of healthcare information in a loss scenario.	Fail to reject null hypothesis
H10	Attainment of a Certified Healthcare Privacy and Security credential is positively associated with reporting future indefinable breaches of healthcare information in a general scenario.	Fail to reject null hypothesis
H11	Attainment of a Certified Healthcare Privacy and Security credential is positively associated with reporting future indefinable breaches of healthcare information in a gain scenario.	Fail to reject null hypothesis
H12	Attainment of a Certified Healthcare Privacy and Security credential is positively associated with reporting future indefinable breaches of healthcare information in a loss scenario.	Fail to reject null hypothesis
H13	Attainment of a Registered Health Information Administrator or Technician credential is positively associated with reporting future indefinable breaches of healthcare information in a general scenario.	Fail to reject null hypothesis
H14	Attainment of a Registered Health Information Administrator or Technician credential is positively associated with reporting future indefinable breaches of healthcare information in a gain scenario.	Fail to reject null hypothesis

	Alternative Hypothesis	Outcome
H15	Attainment of a Registered Health Information Administrator or Technician credential is positively associated with reporting future indefinable breaches of healthcare information in a loss scenario.	Fail to reject null hypothesis

While there was an expected impact on decision-making from percentage of years employed, self-reported knowledge level, and RHIA/RHIT credential, there was not a statistically significant impact in either model and thus fail to reject the null hypothesis for both the general scenarios and the gain scenario.

There was a statistically significant result for higher levels of education within the gain model which indicates that those with higher levels of education, bachelor's and graduate degrees, are less likely than respondents with only a high school or associate's degree, to report a breach with known costs and known benefits of reduced liability and instead choose to take the chance that no costs or corrective actions occur. This is different from the general model which saw no statistical difference between the two groups. While the results from the gain model may seem out of place, they show that those with additional education may feel they have a better understanding of the prompt and/or the reporting guidelines and are willing to take the chance that they are making the correct decision.

There was a statistically significant result for Certified Healthcare Privacy and Security credential within the general model. While the gain model was not significant at the $p<0.05$ level, it was reasonably close with $p=0.053$. This concludes that the CHPS credential was the strongest predictor as it was significant for both models (one at $p<0.05$ and one at $p<0.10$). This

is reiterated with the predicted probabilities which saw CHPS statistically significant at the 0.05 level for both the general and gain breach scenario models.

An individual with a CHPS credential has demonstrated advanced knowledge in the area of privacy. The model results indicate that a respondent with a CHPS is less likely than a respondent without a CHPS to report either a general ambiguous breach or a breach with known costs and known benefits of reduced liability and instead choose to take the chance that no costs or corrective actions occur. This falls in line again with the education level, where more knowledge aligns with the willingness to take a chance.

Research question 2 explored the effects the respondent's reference point based on past reporting had on their choice to report a breach of patient information. The results of the hypotheses testing for research question two are located in Table 29.

Table 29: Hypothesis Testing RQ 2

	Hypothesis	Outcome
H16	Prior reporting of a breach of healthcare information to the Office for Civil Rights is positively associated with reporting future indefinable breaches of healthcare information in a general scenario.	**Reject null hypothesis**
H17	Prior reporting of a breach of healthcare information to the Office for Civil Rights is positively associated with reporting future indefinable breaches of healthcare information in a gain scenario.	Fail to reject null hypothesis
H18	Prior reporting of a breach of healthcare information to the Office for Civil Rights is positively associated with reporting future indefinable breaches of healthcare information in a loss scenario.	Fail to reject null hypothesis

The general scenario found Prior Reporting to be statistically significant, but it was not significant for a gain scenario. This indicates that respondents who had reported a prior breach

were more likely to report an ambiguous breach in the future if they knew little about the incident. However, the statistical difference was not present when participants were provided additional detail and presented with options that included known costs and known benefits of reduced liability or a chance that there might be no costs or corrective actions occur, or high costs and corrective actions. The statistical significance in the general scenario is appropriate as those who have dealt with the process previously may err on the side of caution with little information. However, they may become more discerning when presented with additional information.

Research question 3 explored the effects the framing of the scenario had on the respondent's choice to report a breach of patient information. The results of the hypotheses testing for research question one are located in Table 30.

Table 30: Hypothesis Testing RQ 3

	Hypothesis	Outcome
H19	A breach of healthcare information scenario framed as a gain is positively associated with privacy officers classifying the breach as reportable to the Office for Civil Rights.	**Reject null hypothesis**
H20	A breach of healthcare information scenario framed as a loss is negatively associated with privacy officers classifying the breach as reportable to the Office for Civil Rights.	**Reject null hypothesis**

The chi-square analysis found that the proportion of respondents who would report a breach under a general scenario was statistically different from the proportion of respondents who would report a breach under a gain scenario. The proportion of respondents who would

report a breach under a gain scenario is statistically different from the proportion of respondents who would report a breach under a loss scenario as well. When reviewing the descriptive statistics as the proportion of the respondents visually changes between the three dependent variables. Figure 9 graphically presents this information.

Theoretical Contributions

Based on the literature review and the theoretical models used in this study, the reference point and framing affect the choice a Privacy Officer makes when determining whether to report a breach. This study found that some aspects of a reference point do have an impact on the choice a Privacy Officer makes, including their level of education, types of credentials held, and whether they had reported a previous breach. Other aspects that may compose a reference point were not significant, including the percentage of years worked in healthcare privacy and self-reported knowledge levels. A reference point is a key construct of Prospect Theory under Kahneman and Tversky (1979). The findings from this study indicate support for the construct, that individuals do not take a risk solely on the utility they may receive from the outcome; instead they base the decision relative to a neutral reference point (Kahneman & Tversky, 1979).

The other key construct identified from previous literature is framing, that individuals view and evaluate risk differently when presented with a gain or a loss concept (Kahneman & Tversky, 1979). The findings from this study align with the literature, there is a difference in the way respondents answered based on the framing of the risk. The majority of respondents answered that they would not report when presented with a general scenario with no specifications given to the type of risk. When presented with a gain scenario, this percentage reporting increased and then increased again with a loss scenario.

This study further contributes to the body of literature of Prospect Theory and expands upon the healthcare and management usage of the theory. While not using the latest full iteration of Cumulative Prospect Theory due to constraints, this study did have findings that align with the primary constructs of the theory which are building blocks for future studies. The theory, while still not widely used, can provide a backbone, even in construct form, for decision-making during study formulation.

Practical Contributions

The study findings have practical contributions to the body of knowledge of AHIMA members, Privacy Officers, and breach determination. From a self-reported knowledge level, it is of note that all who participated in the study felt they had at least an average knowledge about privacy, with the majority reporting above average or excellent. At the end of the survey, an area for freeform comments was available, and some write-ins requested additional detail on the scenarios stating that they would need more information to make a decision. This is indicative that the knowledge level of those participating is high, that they understand these decisions generally require further investigation and a certain level of detail. AHIMA can build upon this result by increasing their literature base with articles providing guidance on areas of need and scenario based guidance.

The constructs identified by the theoretical literature impact the practical contributions of the study. It is vital that Privacy Officers understand their reference points and how their framing of an incident can affect their response. Education levels were statistically significant and may indicate a need for higher participation in degree programs by Privacy Officers. This is an area that could be expanded upon to ensure those individuals in a facility making decisions

are fully informed. While there may not be regulations in the federal policies about the qualifications of designated Privacy Officers, AHIMA utilizes educational requirements for their credentials. These requirements should be held firm and potentially increased as further research dictates. AHIMA could also be instrumental in marketing educational requirements to facilities, encouraging employers to hire individuals with higher level degrees. This is already being performed to some extent with the sample job descriptions available in their Body of Knowledge.

There is an indication of a need for Privacy Officer qualifications by the credential results. With the statistical significance of the CHPS credential in both models it lends credence to the value of the advanced knowledge required to obtain the credential and the impact it has on the decision-making process. An interesting finding was that the coding credential was statistically significant. A review of the coding credential domains and subdomains may show specific content that is valuable for Privacy Officers as well. These findings are key for AHIMA and their members. The results are a testament to obtain a credential and they are helpful in marketing credential holders in the marketplace. A focus on compliance aspects of the credentials may be beneficial as well as better ethical standards.

An interesting finding of the study was the demographics of the responses to the three breach scenario questions. When reviewing them at face value outside of the general/gain/loss framing, there was a change in response to the type of scenario. The first scenario was just a basic statement, where the majority responded they would not report. When provided a detailed scenario based on paper records, the majority chose to report. Finally, when provided a detailed scenario based on ransomware the overwhelming majority chose to report. The shift from the

second to the third scenario may indicate a comfort in handling paper privacy concerns and a wariness with technological privacy concerns, especially ransomware. Respondents may have chosen to err on the side of caution due to the ambiguity of ransomware attacks, where the level of compromise to the information may not be as evident.

Privacy officers should review the results of this study carefully and utilize them to enhance their ability to manage breach determinations in their workplace. Higher levels of education, credentials, and knowledge base may enable Privacy Officers to market themselves better in the workplace and enhance their positions within healthcare organizations. Privacy Officers should take advantage of opportunities to increase their exposure to all three of these areas, education, credentials and knowledge base.

The results of this study indicate that breach determination is a case by case basis and dependent on individual decisions. However, healthcare organizations can utilize these results to develop plans with their internal and external stakeholders in the event of a breach of patient information. Implications of a breach are shaped by the type, category, method of access, and number of patients affected, however, it is important to have these high-level plans in place so everyone involved has a basic understanding. Development of these plans should include discussions of when reporting is appropriate and why it is important to report regardless of the consequences.

This recommendation is in line with industry trends. The Emergency Prepardeness and Security Trends in Healthcare survey identified that the third highest safety concern of healthcare organizations is from cyberattacks (RAVE Mobile Safety, 2018). An example of the type of plans needed include the case of Anthem, a healthcare insurance company, who experienced one

of the largest breaches of 2015 and affected 80 million individuals (Keeve, 2016). From that incident the author created a set of lessons companies should consider for a crisis communication plan in the case of a breach of patient information. These lessons include early and easy to understand transparency with the public and authorities which includes a sincere apology and to offer compensation to victims to help re-establish loyalty (Keeve, 2016). As indicated by this study, Privacy Officers need the knowledge and education to assist in the development of these plans.

Policy Contributions

The Office for Civil Rights has previously provided guidance on areas of breach determination; however, the process still has gaps where Privacy Officers are making their own decisions. OCR can use the findings of this study to help identify and address these gaps. Further guidance should be issued to help with the areas of ambiguity and perhaps scenario based guidance as appropriate.

Many comments from the free-form section touched on the need for guidance or new legislation to help clarify areas where the policy has left decisions open-ended. One respondent stated “HIPAA was created in the VCR era. We have a lot more technology, such as smartphones, social media that brings a whole new scope of HIPAA into play”. With the advancements made in technology, federal guidance may have a hard time keeping up due to time constraints in policy creation and revision. Requests for guidance from the open-ended question include definitions for “breach types” and “compromise”; clarify third party right of access and “potential” access.

The current legislation does not have requirements for Privacy Officers outside of the fact that covered entities are required to have a "privacy official." As noted by the findings, education and credentials are significant to decision making and should be considered as standards for Privacy Officers. This is an area that could be expanded upon to ensure those individuals in a facility making decisions are fully informed. Language could be added to the legislation to outline the requirements and/or suggestions for privacy officials in healthcare organizations.

Public Affairs Implications

If a patient's information is stolen from a hacking/IT incident and sold on the blackmarket, a potentially harmful effect is that of insurance fraud and medical identity theft (Korolov, 2015; Federal Trade Commission, 2010). An unauthorized user could expend the patient's available services or the unauthorized user could receive treatment, which ends up on the patient's record as the patient's history (Korolov, 2015; Amori, 2008).

Patient health information is at risk everyday in the United States. The Annual Report to Congress by the Department of Health and Human Services found that in 2016 (the most recent published data), healthcare breaches were reported for almost 27 million patients. While all types of breaches are occurring, the one that affects the most patients per instance is that of hacking/IT incidents. This is concerning as these breaches are occurring more frequently. Per a report from the Office for Civil Rights, the daily ransomware attacks have had a 300% increase from 2015 to 2016 with about 4000 daily attacks (U.S. Department of Health and Human Services, 2016). As stated previously, these types of breaches are difficult to define and only

currently have unofficial guidance from the oversight body, the Office of Civil Rights; meaning facilities are making more and more determinations internally whether to report.

A driving force behind this study was to understand how Privacy Officers make decisions because if they make a wrong decision, it can be extremely detrimental to the patients. The findings from the study indicate that higher knowledge levels of respondents equate to a lower likelihood of reporting, which can be positive for a facility. However, if the case was reportable, it may be harmful to patients. It is essential that the federal government take into account the regulatory burden placed on businesses; however, protecting the privacy of patients must still be a priority.

Several respondents of the study found the language of the federal policy to be confusing or overwhelming. One respondent found it "Difficult to keep up with, especially with sophisticated cyber-attacks and hospitals with little extra money and Human Resources to monitor and protect." It is no surprise that the policy may overwhelmed patients as well. Another respondent stated, "I do believe that for most patients, understanding the HIPAA standards is a difficult task." While the Office for Civil Rights has a 'HIPAA for Individuals' section, if a patient was not familiar with the oversight body or website they may find it difficult to locate or navigate. The patchwork system of federal and state policies, along with the gray areas in the policies, may lead to confusion among patients. This can impact their ability to advocate for themselves and their private information.

Limitations

There are limitations to this study. The first is that there were self-reported measures which may have led to bias in the results. One key variable to monitor was that of Knowledge

Level, where all respondents chose Average or higher, no respondents chose Below Average or Poor. There were also errors in reporting that were corrected by the researcher when cleaning the data. For example, respondents provided ranges for the number of breaches reported and the lowest number of the range was utilized. This also occurred with respondents answering with a '+' sign, for example 300+ breaches. The '+' was removed by the researcher, but the respondent did not provide an accurate number.

One of the key limitations of this study is that the population was restricted to AHIMA members available on the Engage community. This impacts the generalizability of the results. Many Privacy Officers, especially those working in smaller facilities, may not be AHIMA members or hold AHIMA credentials. Future research can hopefully become more inclusive to capture a broader audience to make the results truly generalizable.

While limitations occurred and were accounted for in the study design. The methodology section discusses these in detail as well, but include the inability for a true experimental research design due to ethical concerns (mitigated by design controls) and creation of a survey instrument (mitigated by the use of a pilot study and a subject matter expert).

As evidenced by the descriptive statistics, there was no need to run the third model based on the loss scenario as there was not enough variation in the dependent variable. Research question three still used the data for a bivariate analysis of the framing effects and provided a wealth of information for the theoretical and practical implications, but it was not included in the statistical models.

The subject of the study may have led to non-participation from those contacted. While privacy and ethical concerns were addressed and reviewed by the Institutional Review Board,

potential respondents may not have been allowed, or felt it inappropriate, to participate due to the sensitive nature of the questionnaire or their facility's legal requirements.

Future Research

There are vast areas for future research around these topics. A University of Central Florida team from the Department of Health Management and Informatics (that this researcher participated with) recently published a paper regarding hospital and breach characteristics which received positive attention. The findings of this study may influence that research which is still in progress. A potential future study would be a qualitative review of the free-form comments. This could bring critical areas needing attention forward for federal policy consideration. The qualitative study would be beneficial to the private sector for groups like AHIMA and HIMSS to focus educational initiatives around.

A logical extension of this study would be to distribute the same survey to hospital executives with the American College of Healthcare Executives and/or the Health Information Management Systems Society. This would create an interesting comparison between the employees responsible for reporting and those who would be creating facility policy regarding breach reporting determination. Third-party firms who assist facilities in making breach determinations, such as law offices and consultants may also participate with a similar or modified survey.

Another area of interest for future research would be to explore the patient understanding of breach determination. Many patients may be unaware that this type of determination occurs in facilities or impacts their privacy. Due to the numerous privacy and financial breaches in other sectors, Facebook and Equifax for example, patients may be experiencing fatigue and become

desensitized to notifications. This would help inform policy about the types and level of notifications that need to occur, especially with healthcare information breaches as they can be extremely detrimental as opposed to regular sector breaches.

At the end of 2016, President Barack Obama signed a new policy, the 21st Century Cures Act, into effect (Majumder, Guerrini, Bollinger, Cook-Deegan, and McGuide, 2017). This policy has lofty goals and focuses on rapidly developing treatments for many illnesses through changes to research requirements and information sharing (Majumder et al., 2017). The policy has many benefits including reducing "bureaucratic red tape" in certain areas; however, it may not be as positive for patient privacy as the original authors intended (Hudson, Collings, 2017). As this policy is fairly new, it has not been determined if there is a balance between an individual's privacy and the "insatiable demand for data that's needed to fuel new research" (Buffone, P., 2016). An example of this comes from the Act which provides the director of the National Institute of Health (NIH) to require data sharing from research conducted with funds awarded from NIH (Majumder et al., 2017). This does not seem alarming in a sense due to the general de-identified nature of the data, but researchers found on multiple occasions that de-identified data can be used to identify individuals, especially in the case of genetic information with Direct to Consumer testing providers like 23andME and Ancestry.com (Brase, 2018; Erlich, Shor, Carmi, & Pe'er, 2018). With the onset of this new policy, privacy and the individual patient's understanding of the utilization of their information is an area ripe for research.

Conclusion

The purpose of this study was to explore the impact of personal and organizational knowledge and scenario framing had on the decisions Privacy Officers made in regards to

privacy breach determination. The study used Prospect Theory as a theoretical framework for variable selection and study design. The survey was created with the assistance of a subject matter expert and it was tested using a pilot study. The study targeted individuals with a privacy designation through the AHIMA Engage community. A total of 479 individuals were contacted over several weeks with 170 respondents of which were 123 full surveys. After data collection and cleaning, statistical software was used to run multiple analyses with significant results. The findings of the study supported the theoretical framework and provided industry and public affairs implications.

Healthcare privacy is paramount due to the sensitive nature and amount of information collected by care providers. Even though there are federal and state policies in place to protect individual patient privacy, the findings of this study show that there is a gap where Privacy Officers have to make their own decisions, and there is a difference in the types of decisions they are making on a day to day basis.

With the significant results of the paper identified as education level, credential level, and scenario-based, they are indicative of a need for educational opportunities and potential requirements for designated Privacy Officers. This includes initial levels of education as well as continuing education requirements to ensure the individuals stay up to date on the current trends and threats in healthcare. Educational initiatives may also be beneficial at the executive level as these individuals may underestimate the importance of privacy initiatives which could lead to underreporting of breaches. These educational initiatives may include scenario based training to identify areas of concern and confusion for their organization. This can assist in developing well-round policies and procedures for breach reporting. Future research at the executive level

of understanding and decision-making is crucial for policy implications. Both levels, Privacy Officer and executive positions, would benefit from scenario-based educational opportunities as well.

Healthcare has a variety of settings, from small individual physician practices to large national integrated delivery systems. The types of care vary from basic preventative care to high impact invasive treatment. These varieties of settings and care provision lead to difficulties in identifying a single answer to protecting patient information. The types of systems and information processes used among these is more a best of fit than a best of breed for this reason. Future guidance and policies need to address these gaps and can use the insight provided by this study of areas that influence the decision-making process.

APPENDIX A: INITIAL SURVEY EMAIL

Subject: Survey Participation Request

Message:

Good Morning/Afternoon/Evening,

My name is Amanda Walden and I am a doctoral student at the University of Central Florida. I am currently conducting research for my dissertation to evaluate the decision-making process of Privacy Officers in regards to breach notification. As you are listed on the AHIMA Engage community with a Privacy title, I am inviting you to participate in this research study by completing the survey. Please copy and paste address to use in your desired browser:

http://bit.ly/Privacy_Officer_Survey

The following questionnaire will require approximately 10 minutes to complete. The survey is anonymous and the results will be publicly reported in aggregate format only. Participation is strictly voluntary and you may refuse to participate at any time.

Thank you for taking the time to assist in my educational endeavors.

If you require additional information or have questions, please contact me at the number listed below.

Thank you for your time and consideration.

Sincerely,

Amanda M. Walden, PhD Candidate
MSHSA, RHIA, CHDA
(407) 823-3613
Amanda.walden@ucf.edu

College of Health and Public Affairs
University of Central Florida
4364 Scorpius Street
Orlando, FL 32816-2205

Reviewed by UCF IRB 10/27/17
UCF IRB
407-823-2901
407-882-2012
irb@ucf.edu

Dissertation Chair: Kendall Cortelyou-Ward
kendall.cortelyou-ward@ucf.edu
(407) 823-2359

APPENDIX B: FIRST REMINDER EMAIL

Subject: Privacy Officer Survey

Message:

Good Morning/Afternoon,

Two weeks ago I sent an e-mail asking you to complete a survey about the decision-making process of Privacy Officers in regards to breach notification. I received 68 participants and the quality of the data and responses was outstanding. If you completed the survey, thank you very much!

Unfortunately to have an effective model I need at minimum 115 responses. If you have not already completed the survey, I ask that you please consider participating. It should only take about 10 minutes to complete. Simply click the link below to begin answering the questions.

http://bit.ly/Privacy_Officer_Survey

A reminder that the survey is anonymous and the results will be publicly reported in aggregate format only. Participation is strictly voluntary and you may refuse to participate at any time.

If you require additional information or have questions, please contact me at the number listed below.

Thank you for your time and consideration.

Sincerely,

Amanda M. Walden, PhD Candidate
MSHSA, RHIA, CHDA
(407) 823-3613
Amanda.walden@ucf.edu

College of Health and Public Affairs
University of Central Florida
4364 Scorpius Street
Orlando, FL 32816-2205

Reviewed by UCF IRB 10/27/17
UCF IRB
407-823-2901
407-882-2012
irb@ucf.edu

Dissertation Chair: Kendall Cortelyou-Ward
kendall.cortelyou-ward@ucf.edu
(407) 823-2359

APPENDIX C: FINAL REMINDER EMAIL

Subject: Privacy Officer Survey

Message:

Good Morning/Afternoon,

I am writing to follow-up on the request I sent asking you to participate in a survey regarding the decision-making process of Privacy Officers in regards to breach notification. If you completed the survey, thank you very much! This survey is drawing to a close, and I am still a few participants short.

If you have not already completed the survey, I ask that you please consider participating. It should only take about 10 minutes to complete. Simply click the link below to begin answering the questions.

http://bit.ly/Privacy_Officer_Survey

A reminder that the survey is anonymous and the results will be publicly reported in aggregate format only. Participation is strictly voluntary and you may refuse to participate at any time.

If you require additional information or have questions, please contact me at the number listed below.

Thank you for your time and consideration through this process.

Sincerely,

Amanda M. Walden, PhD Candidate
MSHSA, RHIA, CHDA
(407) 823-3613
Amanda.walden@ucf.edu

College of Health and Public Affairs
University of Central Florida
4364 Scorpius Street
Orlando, FL 32816-2205

Reviewed by UCF IRB 10/27/17
UCF IRB
407-823-2901
407-882-2012
irb@ucf.edu

Dissertation Chair: Kendall Cortelyou-Ward
kendall.cortelyou-ward@ucf.edu
(407) 823-2359

APPENDIX D: FORMAL QUESTIONNAIRE LETTER

Risk in Privacy Breach Determination among Privacy Officers

Date

Dear Participant:

My name is Amanda Walden and I am a doctoral student at the University of Central Florida. I am currently conducting research for my dissertation. The purpose of this research is to evaluate the decision-making process of Privacy Officers in regards to breach notification. As you are listed on the AHIMA Engage community with a Privacy title, I am inviting you to participate in this research study by completing the linked survey.

The following questionnaire will require approximately 10 minutes to complete. There is no compensation for responding and the study has been reviewed by University of Central Florida Institutional Review Board for known risk. The survey is anonymous and the results will be publicly reported in aggregate format only. In order to ensure that all information will remain confidential, please do not include your name or your organization's name. Participation is strictly voluntary and you may refuse to participate at any time. If you choose to participate, please answer all questions as honestly as possible.

Thank you for taking the time to assist in my educational endeavors. The survey results will primarily be used for recommendations for current and future federal legislation regarding healthcare privacy breach reporting.

Completion of the questionnaire will indicate your willingness to participate in this study. If you require additional information or have questions, please contact me at the number listed below. This study is being conducted under the direction of Dr. Kendall Courtelyou-Ward at the University of Central Florida. Please feel free to contact her if you have any questions or concerns (anonymously if you so choose) regarding the manner in which this study is being conducted. She can be reached at (407) 823-2359 or by e-mail at kendall.cortelyou-ward@ucf.edu

Sincerely,

Amanda M. Walden, PhD Candidate
MSHSA, RHIA, CHDA
(407) 823-3613
Amanda.walden@ucf.edu

College of Health and Public Affairs
University of Central Florida
4364 Scorpius Street
Orlando, FL 32816-2205

Reviewed by UCF IRB 10/27/17
UCF IRB Phone: 407-823-2901 & 407-882-2012 Email: irb@ucf.edu

APPENDIX E: QUESTIONNAIRE

As you answer this survey, please respond keeping your ***current*** facility in mind.

Screening Question:

1. Are you currently employed?
    a. Yes
    b. No – Conclude Survey

2. Are you the current designated Privacy Officer for your facility?
    a. Yes
    b. No - Conclude Survey

3. Date of Survey Completion:_____

4.What is your Age (in years)? Continuous.

5.What is your Gender?:

a. Male
b. Female
c. Other
d. Prefer not to disclose

6.Select your highest completed level of education:

a. High School
b. Associate's Degree
c. Bachelor's Degree
d. Master's Degree
e. Doctoral Degree

7.Select all AHIMA credentials that you are currently certified to hold:

a. RHIA- Registered Health Information Administrator
b. RHIT- Registered Health Information Technician
c. CCA- Certified Coding Associate
d. CCS- Certified Coding Specialist
e. CCS-P- Certified Coding Specialist- Physician-based
f. CDIP- Certified Documentation Improvement Practitioner
g. CHDA- Certified Health Data Analyst
h. CHPS- Certified in Healthcare Privacy and Security
i. CHTS- Certified Healthcare Technology Specialist
j. CPHI- Certified Professional in Health Informatics

8.Your Privacy role in your current facility falls into which of the following departments, choose only one.

a. Executive Team
b. HIM Department
c. IT Department
d. Joint HIM/IT Appointment
e. Other - Text Box for fill-in

9. Is your facility located in a state with additional healthcare specific privacy breach notification laws?)

States with additional healthcare specific privacy breach notification laws are as follows:

Arkansas
California
Delaware
Florida
Illinois
Kentucky
Maryland
Missouri
Montana
Nevada
New Hampshire
North Dakota
Oregon
Rhode Island
Texas
Wyoming

a. Yes
b. No

10. How would you classify your healthcare facility?
    a. Acute Care Hospital
    b. Ambulatory Surgery Center
    c. Behavioral/Mental Health
    d. Clinic/Physician Practice
    e. Consulting Service
    f. Education
    g. Health Information Exchange
    h. Home Health/Hospice
    i. Integrated Healthcare Delivery System
    j. Long Term Care
    k. Non-Provider Setting (e.g., govt., vendor, assoc.)
    l. Other Provider Setting (e.g., rehab)
    m. Regional Extension Center

11. What is the profit status of your healthcare facility?
    a. Non-Profit
    b. For-Profit

12. How many years have you been employed in the healthcare field? – Continuous

13. How many years have you been employed in the healthcare privacy field? – Continuous

14. How would you rate your knowledge of healthcare privacy?
    a. Excellent
    b. Above Average
    c. Average
    d. Below Average
    e. Poor

15. During your time at your current employer, has your facility reported a breach of Protected Health Information (PHI) to the Office for Civil Rights?
    a. Yes
    b. No- Skip to Question 19

16. During your time at your current employer, how many breaches of patient Protected Health Information (PHI) has your facility reported to the Office for Civil Rights? – Continuous

17. What classification were the breaches indicated in the previous question?
    a. Fewer than 500 patients per incident ONLY
    b. More than 500 patients per incident ONLY
    c. Cases of both 'Fewer than 500 patients per incident' and 'More than 500 patients per incident'

18. What were the outcomes of the breaches from the Office for Civil Rights? Choose all that apply.
    a. Corrective Action Plan
    b. Criminal Penalties
    c. OCR Fine
    d. None

19. If a breach of patient PHI occurs in the future that is not clearly identified as reportable, will you report or not report?
    a. Report
    b. Not Report

20. Your healthcare facility was unlawfully entered. The individual who broke in potentially had access to 450 paper patient records that were held in that office. There were no security cameras to record events, although office supplies were gone through, only a printer with no PHI was taken. Your policies and procedures are up to date, however they do not specifically address breach determination for break-in for your facility. All policies, procedures, training and risk assessment and management are in compliance.

Your next step is to review the four factor risk assessment to determine if the potential breach is reportable to the patients and the Office for Civil Rights. Upon review:

1) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification. – The records are paper based and included multiple types of unsecured PHI including sensitive patient identifiers.
2) The unauthorized person who used the PHI or to whom the disclosure was made. – The unknown individual who broke into the facility was not authorized to view the records and their intent is unknown.
3) Whether the PHI was actually acquired or viewed. – Employees cannot distinguish if the records have been disturbed, accessed or read.
4) The extent to which the risk to the PHI has been mitigated. – No records were missing.

Choose one of two options, ‘report’ or ‘do not report’.

If you report, you will bear the cost of reporting but your facility benefits by having your liability reduced.

If you do not report one of 2 options occur. (A) OCR investigates for any other reason, may find your facility made an inappropriate determination, fines and/or corrective actions of unknown levels may be made. OR (B) OCR does not investigate this incident and your facility benefits by incurring no costs or corrective actions.

a. Report
b. Not Report

21. An employee at your facility clicked on a link from a Phishing e-mail which led to a ransomware attack on your facility. Payout was required and access was restored to your system. The attacker potentially had access to 750 unsecured (unencrypted) patient records in the system. All policies, procedures, training and risk assessment and management are in compliance.

Your next step is to review the four factor risk assessment to determine if the potential breach is reportable to the patients and the Office for Civil Rights. Upon review:

1) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification. – The records are electronic based and included multiple types of unsecured PHI, including patient identifiers.

2) The unauthorized person who used the PHI or to whom the disclosure was made. – The attacker was not authorized to view the records. No idea of whether other malware was left behind.

3) Whether the PHI was actually acquired or viewed. – The system cannot distinguish if records were viewed or copied.

4) The extent to which the risk to the PHI has been mitigated. – malware infection was removed and PCs reformatted and reloaded.

Choose one of two options, 'report' or 'do not report'.

If you report, there are negative public relations consequences from media reporting and the incident posted on the OCR website but there is no real possibility of a fine.

If you do not report one of 2 options occur. (A) OCR does not investigate this incident and your facility incurs no costs/corrective actions/negative public relations. OR (B) A compliant or other reason allows OCR to open an investigation where they review the breach determination and decide it was improper, with potentially large fines being issued with resulting negative media exposure and increased public relations issues.

a. Report
b. Not Report

22. The April 2017 cover story for the Journal of AHIMA was titled “Is HIPAA Outdated?” What are your thoughts regarding the HIPAA legislation in terms of breach notification and its ability to adapt? Please add any additional comments regarding breach notification that you feel would be useful to this study.

APPENDIX F: IRB OUTCOME LETTER 1

University of Central Florida Institutional Review Board
Office of Research & Commercialization
12201 Research Parkway, Suite 501
Orlando, Florida 32826-3246
Telephone: 407-823-2901 or 407-882-2276
www.research.ucf.edu/compliance/irb.html

Approval of Exempt Human Research

From: **UCF Institutional Review Board #1**
FWA00000351, IRB00001138

To: **Amanda M Walden**

Date: **October 27, 2017**

Dear Researcher:

On 10/27/2017, the IRB reviewed the following activity as human participant research that is exempt from regulation:

Type of Review:	Exempt Determination
Project Title:	RISK IN PRIVACY BREACH DETERMINATION: THE APPLICATION OF PROSPECT THEORY TO HEALTHCARE PRIVACY OFFICERS
Investigator:	Amanda M Walden
IRB Number:	SBE-17-13440
Funding Agency:	
Grant Title:	
Research ID:	N/A

This determination applies only to the activities described in the IRB submission and does not apply should any changes be made. If changes are made and there are questions about whether these changes affect the exempt status of the human research, please contact the IRB. When you have completed your research, please submit a Study Closure request in iRIS so that IRB records will be accurate.

In the conduct of this research, you are responsible to follow the requirements of the Investigator Manual.

On behalf of Sophia Dziegielewski, Ph.D., L.C.S.W., UCF IRB Chair, this letter is signed by:

Signature applied by Renea C Carver on 10/27/2017 03:15:33 PM EDT

Designated Reviewer

APPENDIX G: IRB OUTCOME LETTER 2

University of Central Florida Institutional Review Board
Office of Research & Commercialization
12201 Research Parkway, Suite 501
Orlando, Florida 32826-3246
Telephone: 407-823-2901 or 407-882-2276
www.research.ucf.edu/compliance/irb.html

Determination of Exempt Human Research

From: **UCF Institutional Review Board #1**
FWA00000351, IRB00001138

To: **Amanda M Walden**:

Date: **February 06, 2018**

Dear Researcher:

On 02/06/2018, the IRB reviewed the following activity as human participant research that is exempt from regulation:

Type of Review:	Exempt Determination, Category 2
Modification Type:	Added follow-up recruitment email
Project Title:	RISK IN PRIVACY BREACH DETERMINATION: THE APPLICATION OF PROSPECT THEORY TO HEALTHCARE PRIVACY OFFICERS
Investigator:	Amanda M Walden
IRB Number:	SBE-17-13440
Funding Agency:	
Grant Title:	
Research ID:	N/A

This determination applies only to the activities described in the IRB submission and does not apply should any changes be made. If changes are made and there are questions about whether these changes affect the exempt status of the human research, please contact the IRB. When you have completed your research, please submit a Study Closure request in iRIS so that IRB records will be accurate.

In the conduct of this research, you are responsible to follow the requirements of the Investigator Manual.

This letter is signed by:

Renea Carver

Signature applied by Renea C Carver on 02/06/2018 04:35:05 PM EST

Designated Reviewer

APPENDIX H: DIRECTOR LEVEL PRIVACY DESIGNATION BY STATE

State	'Privacy'	Total Members
Alabama	9	79
Alaska	3	16
Arizona	8	90
Arkansas	6	70
California	32	383
Colorado	7	102
Connecticut	8	40
Delaware	0	13
DC	1	8
Florida	31	300
Georgia	13	144
Hawaii	1	15
Idaho	3	29
Illinois	21	250
Indiana	15	135
Iowa	6	63
Kansas	5	111
Kentucky	9	102
Louisiana	10	117
Maine	4	25
Maryland	10	104
Massachusetts	25	113
Michigan	17	135
Minnesota	8	113
Mississippi	6	66
Missouri	15	122
Montana	2	23
Nebraska	4	56
Nevada	4	53
New Hampshire	4	27
New Jersey	10	114
New Mexico	2	31
New York	15	293
North Carolina	12	160
North Dakota	2	29
Ohio	21	186
Oklahoma	9	86
Oregon	5	40
Pennsylvania	15	261
Rhode Island	1	17
South Carolina	5	69
South Dakota	1	37
Tennessee	17	219
Texas	29	420
Utah	4	32
Vermont	2	17
Virginia	7	104
Washington	16	96
West Virginia	7	45
Wisconsin	11	118
Wyoming	1	15
Total	479	5293

APPENDIX I: QUESTIONNAIRES DELETED DUE TO MISSING DATA

Question Number	Deleted responses	Reasoning
0	6	Surveys did not answer all or majority of questions
1	5	Respondents answered ‘No’
2	5	Respondents answered ‘No’
3	6	Respondents did not answer
9	1	Respondents did not answer
11	3	Respondents did not answer
13	1	Respondents did not answer

APPENDIX J: PILOT STUDY FEEDBACK

Feedback: Comments/Concerns on Questions - For Pilot Study
Should reach outside the limits of AHIMA, there are many non-traditional Health Care settings that follow the Privacy rules. Provide more options other then report/do not report more information and other tools are available to determine if it should be reported .
I would like to see a comments box on the 'If a breach of patient PHI occurs in the future and is not clearly identified as reportable"... In my current environment, we seek outside Legal Privacy Counsel to walk through the Breach Assessment and ensure an impartial party is helping with the determination. This is the trend that I see in Privacy and Security, where requests for outside expertise from a reputable organization is working with your company to ensure an unbiased resolution to assessments.
Great study that confirmed some of my thoughts - First, I would have let my moral compass, ethics and instincts drive my decisions concerning breach notifications (i.e., I would want to do the right thing for a particular incident, and I would want to work in organizations with that same culture); and HIPAA, and the liabilities it would present would be my second thought. However, I do appreciate that nationally, HIPAA increased public awareness and discussions of the importance of patient privacy and confidentiality concerns in the age of the EHR.

APPENDIX K: SURVEY COMMENTS

I don't think the breach notification and reporting rules are having any impact on breaches. They were originally designed to shame organizations who weren't careful with PHI but we are seeing that even the most secure organizations (including the organizations test with enforcing The rules) are unable to keep PHI safe. Energy should be going into best practices for that (not to mention the considerable investment involved) and less to a strategy that isn't working

Additional clarity is needed around determining if a breach is reportable.

As an HIE/Community Wide Clinical Data Repository, suspected breaches are typically reported to the institution who originated/contributed data to the HIE. We facilitate investigation and provide all documentation necessary for the covered entity to make these determinations and report if they determine that a reportable breach has occurred.

Breach notification assessment is too subjective.

Clearer guidance needs to be published as the risk assessment and process is still subjective. Consumers are also becoming immune to reports as they may receive many letters that there "may be" a breach but it could not be validated. Organizations may send a letter to the patient as a "heads up" even though the organization has determined it does not fully meet the breach notification requirements.

Cumbersome but necessary - cyber attacks are concerning - government mandates for quality programs take away money that could be spent to help assess / prevent risks related to breaches - it is a catch 22.

Cumbersome with minimal guidance when needing to determine breach notification.

Definite need to update. Need to remove the accounting with the exception of inappropriate. Need to clarify the 3rd party right to access. Need to remove patient right to access for TPO. Many of the rules are more so up for interpretation vs. clear

definition of compromise is still needed

Difficult to keep up with, especially with sophisticated cyber attacks and hospitals with little extra money and Human Resources to monitor and protect.

Guidance on "potential" access is needed. A compromised system does not mean data was accessed. A technical risk assessment would need to be conducted with forensic analysis.

Additionally, a physical risk assessment would need to be done as in the example of the PHI left out and someone stole office supplies. There has to be reasonable evidence that the information was disclosed for a breach to be investigated.With the latest malware that do not have a storage-footprint, then we probably all can assume one is floating around collecting / inspecting information. Should we all declare a breach? Security is based on reasonable assurance. So should breaches. That's where HHS needs to catch up. Also, provide better guidance documents -- although now the DOJ apparently can't use guidance documents. Too much confusion all around on this.

HIPAA is alive and well; separate State regulation can be difficult when communicating with agencies who do not understand HIPAA. Further defined breach types and the notification process would be welcomed.

HIPAA is and always has been too vague to adhere to with any degree of certainty

HIPAA is outdated, especially in regard to the punitive nature of breach reporting.

HIPAA legislation needs to be updated and additional clarification should be added regarding the 4-factor assessment and reporting requirements. OCR is behind on review of cases and needs to find a way to provide more timely feedback to incidents reported that affect 500+ individuals.

HIPAA needs to be updated to reflect the electronic world in which we live. And, there has always been tension between protection of patient information and sharing it as promoted by other data use initiatives by the government. There needs to be more clarification regarding how Office of Civil Rights would view some of these electronic scenarios so that hospitals, clnics etc. will be informed and can act accordingly.

HIPAA needs updating.

HIPAA under appreciates the pediatric patient; there are a number of instances where pediatric issues are not addressed directly. Nancy Davis's comments on HIPAA and clarifications on patient portals is spot on; especially in a pediatric populations.

HIPAA was created in the VCR era. We have a lot more technology, such as smart phones, social media that brings an whole new scope of HIPAA into play.

I agree that with the continuous advancing technology we are struggling with inappropriate use of cell phones, photos, text messages, instant messaging etc. It will require more direction from the OCR to get better compliance from clinicians and providers wanting to utilize these methods of communication for patient care.

I am frustrated that I must spend countless hours logging and notifying patients for things such as misdirected faxes, employee snooping and other bad behaviours that result in few persons PHI being exposed. I think that this should be a hospital HR policy and leave the

feds out of it. I agree that breaches involving a large amount of patients needs to be investigated, mitigated and reported. The fines are unnecessary. I agree with corrective action plans. The regulations are very difficult to follow and as usual government regulations leave too much ambiguity that results in much time and money being spent determining how to handle countless ill defined situations. Health care organizations are struggling. To spend hours investigating why someone misdirected a fax is insane. In addition, we reported annually our breaches, less than 500, abiding by the law and now we are the focus of a full blown investigation that has been gong on for 2 years. This after we spent $150,000 on software to "meet HIPAA security standards". Seems that following the rules gets you punished. I suspect that if OCR looked at every covered entity they would find infractions worthy of their fines. Bottom line, they should offer more educational and clarity on HIPAA and less punishment. The regulations lend themselves to sure failure this may be by design.

I appreciate that patient information needs to be kept private. I do think the HIPAA laws could stand to be revised, however. It's not 'out-dated' per-say, but could use fine-tuning.

I believe it is necessary, but needs to be tweaked with the rising security breaches.

I believe there were improvements with Omnibus and breach notification which made assessment more objective and consistent (ie., four factor analysis), and provided a method for good documentation about how privacy officers reached their conclusions.
Additional comments:
Below is some input about a few of the questions asked in this survey.

With limited knowledge of the incident, if a breach of patient PHI occurs in the future that is not clearly identified as reportable by a four-factor risk analysis, will you report or not report?
Need more info/definition of what you mean with â€œclearly identified as reportableâ€• . Are you meaning â€œlow compromiseâ€• ? It is difficult to select an answer of report or not report without more information. It is all driven by the 4 factor analysis/ data compromise which still has a subjective component. I went with â€œclearly identifiedâ€• as I cannot conclude that the incident resulted in low compromise of data so I would report it.

An employee at your facility clicked on a link from a Phishing e-mail which led to a ransomware attack on your facility. Payout was required and access was restored to your system. The attacker potentially had access to 750 unsecured (unencrypted) patient records in the system. All policies, procedures, training and risk assessment and management are in compliance.
Need more information about whether the records were exfiltrated from the facility "determined by forensics and type of ransomware, etc. And what does attacker potentially had access to 750 unsecure (unencrypted) patient records? How? I am worried that some

may read access and select to report, however, without knowing the forensics/other info, this may not be a reportable breach. Also see OCR guidance on breach notification and ransomware to make things even more interesting!

I believe they are outdated, but Patient Privacy has come a long way, since I first was introduced to it.

I do believe that breaches in healthcare are still under-reported. I would find it interesting what peoples' opinion were of the OCR and its ability to enforce this behemoth called Breach Notification.

I do believe that for most patients, understanding the HIPAA standards is a difficult task. However, from a provider point of view, I feel that the standards protect the patient's information well. I would prefer that both state and federal laws be the same, and also prefer that the standards apply to all who have access to PHI, including providers who do not accept insurance. I think technology has outpaced some of the HIPAA provisions, but overall it has served its purpose. I foresee additional privacy laws on the horizon as technology advances, but I feel that a complete overhaul of HIPAA is unnecessary.

I do not believe HIPAA is outdated; I believe more rules should be put in to place.

I do not think HIPAA is outdated, since its provisions remain relevant.

I don't think it is outdated, but hard for the average small clinic to comply. It is hard to understand and leaves the uninformed with fear and guilt as motivators. This will cause issues regardless of the scenario. Most small clinics do nothing or utilize firms that specialize in cut and paste forms. The clinic is hard pressed to know if they are clearly following the law. AND the clinic is responsible ultimately for knowing.

I feel that phishing and cyberattacks are not fully able to be vetted through the current four-step process very well. We, as an inpatient acute care, locked psychiatric hospital are host to different types of attacks than normal hospitals and often find ourselves in deep discussion and workgroups going over what does and does not constitute a threat/risk. It would great to have more defined guidelines to use. Also, I have not found very much by way of support on AHIMA for these incidents. Something like a chat board or venue to discuss them would be greatly beneficial, especially since many Privacy Officers are wearing other hats and performing other roles and Privacy Officer is just one of their duties. Having a community of others to vet things with would be awesome!

I feel the criteria to evaluate a breach is not clear and depending on who is evaluating it, can choose not to report because the person evaluating it might feel that the information is not compromised where another would see it different. One person feels if a person has anothers PHI in their hands and reads it, it is a breach even though the person chose to bring

it back where another viewing it might feel its a low compromise and not report it. It is very unclear in evaluating and I feel could definitely be improved.

I have read that a bill has been proposed to reduce the time allowed for notification of breach to the patient. It takes time to investigate incidents, especially when it can involve out of state breaches.

I think it is outdated and the requirements are getting more cumbersome and draconian to implement and maintain compliance.

I think its confusing for everyone and no one really fully understands

I think the breach notification requirements are sufficient.

I think the notion of HIPAA is outdated as any person working within health facilities understands the importance of confidentiality and privacy. Even with breach notification being a cumbersome process, I believe in this day and age of identity theft it is a necessary evil.

If there is access to electronic records, an analysis of risk should not apply. It should be considered a breach.

It appears OCR only address breaches involving more than 500 patients and bypass individual breaches.
I feel we need more detailed guidelines as far as exact procedures/practices on how to protect PHI. For example, Athena does not segregate super-confidential information, nor do their reports indicate if a staff member views a patient chart on a need to know basis. Athena reports will only indicate entries made in the chart by staff. I did a test run and viewed HIV lab results, psychotherapy notes, routine office visits, etc. and Athena reports only indicate the date and time I opened the patient chart but does not indicate the documents I viewed nor the time I exited the chart. I receive patient complaints concerning staff breaching their records but I cannot obtain valid documentation to support or deny their allegations. Fed regs need to establish and enforce more strict guidelines on protecting patents civil rights to privacy.

Outdated definitely. Very broad determinations.

Policy makers are not in the trench of privacy breach notification and don't truly understand what a patient is going to do when we notify them of breach.

Potential for access does not mean the user was trying to acquire PHI, typically ransomware and physical break ins are attributed the "items" of value (Rxs, equipment, supplies) not PHI. Many times people that conduct these unfortunate events do not understand the value of what they have in front of them.

Reportable breaches to OCR should be limited to significant incidents.

See both sides. I feel its important to notify one who's privacy may be at risk so they can respond appropriately, however this can easily backfire to cause much more harm than the actual breach may ever cause. Each case is quite individual and should be evaluated accordingly. Then rational judgment exercised in deciding to report and notify.

since the regulations were implemented in 2003 and 2005, with limited updates in 2013. I believe some significant revisions need to take place to the regulations in order to provide more specific guidance to covered entities.

The Breach Notification is outdated and we need defined reportable measures now that we are totally electronic. The Omnibus Hi Tech Rule did not update breach notification

The HIPAA legislation in terms of breach notification and its ability to adapt are appropriate and feel the patient safety and patient's PHI security should be top priority.

The HIPAA policy could definitely use an update. Technology has significantly advanced since the law was enacted.

There is a gray area in HITECH's reporting rules that makes it difficult to determine exactly what is required. Privacy professionals are in a tough spot when they take a "gray area" scenario to administration. What is even tougher is balancing HITECH breach reporting rules with state rules. If there were a federal rule I could see all breach notification rules rolling in to one regulation.

There is a lot of grey areas relating to HIPAA and breach notification.

thorough investigation of each incident must be done to determine potentials of a breach, all facts must be assessed and a team should determine need to report vs one person

to me HIPAA is ever changing and growing and anyone in the field of Privacy should always stay as current and on top of matters as possible. I do not feel HIPAA is outdated, but I feel that information given in the realm of the workplace and society is outdated.

Too far over-reaching and impractical.

Unfortunately, current legislation has not caught up to technological advances and risks.

We have been dealing with Privacy in healthcare for years before HIPAA was enacted. We have adapted throughout the years to assure that we are always maintaining privacy of patients as well as our workers. HIPAA did not change this in any way, it just made things a little more difficult to weed through the true breaches vs. the incidentals.

When performing my OCR notification assessment I also consider the reaction of the patient when notified of the breach.

While the risk of harm analysis was changed, the low probability of compromise analysis is basically the same. It's still pretty subjective and based on whether the individuals doing the assessment think anyone could do anything harmful to the subject individuals.

You should always report an incident

Your scenarios are good but lack key information, #2- if facility was up to date physical safeguards for records after hours holding and nothing left on desk would have been minimal plan. #3 systems review by IT would be able to assess large volume movement file to external IP, addressing if the files were in fact compromised... great study and yes we must keep instep with IT advancements to ensure privacy for our clients. OCR continues to lean towards over reporting.

APPENDIX K: COPYRIGHT PERMISSIONS

Copyright Clearance Center

Note: Copyright.com supplies permissions but not the copyrighted content itself.

1 PAYMENT 2 REVIEW **3 CONFIRMATION**

Step 3: Order Confirmation

Thank you for your order! A confirmation for your order will be sent to your account email address. If you have questions about your order, you can call us 24 hrs/day, M-F at +1.855.239.3415 Toll Free, or write to us at info@copyright.com. This is not an invoice.

Confirmation Number: 11746215
Order Date: 09/06/2018

If you paid by credit card, your order will be finalized and your card will be charged within 24 hours. If you choose to be invoiced, you can change or cancel your order until the invoice is generated.

Payment Information

Amanda Walden
amzak@knights.ucf.edu
+1 (407) 823-3613
Payment Method: n/a

Order Details

JOURNAL OF RISK AND UNCERTAINTY

Order detail ID: 71531797
Order License Id: 4423150591228

ISSN: 0895-5646
Publication Type: Journal
Volume:
Issue:
Start page:
Publisher: SPRINGER NEW YORK LLC

Permission Status: Granted
Permission type: Republish or display content
Type of use: Thesis/Dissertation

Requestor type	Academic institution
Format	Print, Electronic
Portion	chart/graph/table/figure
Number of charts/graphs/tables/figures	1
The requesting person/organization	Amanda Walden
Title or numeric reference of the portion(s)	Figure 3
Title of the article or chapter the portion is from	Advances in Prospect Theory: Cumulative Representation of Uncertainty
Editor of portion(s)	N/A

Author of portion(s)	Tversky & Kahneman
Volume of serial or monograph	5
Issue, if republishing an article from a serial	4
Page range of portion	313
Publication date of portion	1992
Rights for	Main product
Duration of use	Life of current edition
Creation of copies for the disabled	no
With minor editing privileges	no
For distribution to	United States
In the following language(s)	Original language of publication
With incidental promotional use	no
Lifetime unit quantity of new product	Up to 499
Title	RISK IN PRIVACY BREACH DETERMINATION: THE APPLICATION OF PROSPECT THEORY TO HEALTHCARE PRIVACY OFFICERS
Instructor name	Amanda Walden
Institution name	University of Central Florida
Expected presentation date	Oct 2018

Note: This item will be invoiced or charged separately through CCC's **RightsLink** service. More info **$ 0.00**

This is not an invoice.

Total order items: 1 **Order Total: 0.00 USD**

RE: Permission for Journal Figures

Davies, Orla <odavies2@wiley.com>

Mon 9/24/2018 7:14 AM

To: Amanda Walden <Amanda.Walden@ucf.edu>;

Dear Amanda,

Thank you for your email.

Permission is granted for you to use the material requested for your thesis/dissertation subject to the usual acknowledgements (author, title of material, title of book/journal, ourselves as publisher) and on the understanding that you will reapply for permission if you wish to distribute or publish your thesis/dissertation commercially.

You should also duplicate the copyright notice that appears in the Wiley publication in your use of the Material. Permission is granted solely for use in conjunction with the thesis, and the material may not be posted online separately.

Any third-party material is expressly excluded from this permission. If any material appears within the article with credit to another source, authorisation from that source must be obtained.

Many thanks,

Orla Davies
Rights Assistant
John Wiley & Sons Ltd

WILEY

From: Wiley Global Permissions
Sent: 14 September 2018 11:44
To: Amanda Walden <Amanda.Walden@ucf.edu>
Subject: RE: Permission for Journal Figures

Hi Amanda,

I have received your email and will look into this for you now. I will get back to you in due course.

Many thanks,

Orla Davies
Rights Assistant
John Wiley & Sons Ltd

WILEY

From: Amanda Walden [mailto:Amanda.Walden@ucf.edu]
Sent: 13 September 2018 19:47
To: Wiley Global Permissions <permissions@wiley.com>
Subject: Permission for Journal Figures

Good Afternoon,

I am trying to obtain permissions for 2 figures from the same journal article to use in a dissertation. I went through the JSTOR link and it allowed me to fill out an application through the Copyright Clearance site. However it stated that the rights were not available. After speaking with their customer assistance line they directed me to speak with you. I am hoping you can assist or direct me to the correct place.

The paper is Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision under risk. *Econometrica: Journal of the Econometric Society*, *47*(2), 263-291.

Thank you for your assistance,

Amanda Walden, MS-HSA, RHIA, CHDA
Instructor
University of Central Florida
Health Management & Informatics
4000 Central Florida Blvd.
HPA II, Room 218
Orlando, FL 32816-2205
Office: 407-823-3613

Amanda Walden, MS-HSA, RHIA, CHDA
Instructor
University of Central Florida
Health Management & Informatics
4000 Central Florida Blvd.
HPA II, Room 218
Orlando, FL 32816-2205
Office: 407-823-3613

REFERENCES

Adler-Milstein, J., Green, C., Bates, D. (2013). A survey analysis suggests that electronic health records will yield revenue gains for some practices and losses for many. *Health Affairs 32*(3). 562-570.

AHC Media LLC. (2016). Hackers target hospitals with "ransomware". *ED LEGAL LETT. 27*(4): 1-4.

AHIMA (2013a). Analysis of modifications to the HIPAA privacy, security, enforcement, and breach notification rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; other modifications to the HIPAA rules. Retrieved 4 June 2014 from https://library.ahima.org/PdfView?oid=106127

AHIMA (2013b). Performing a Breach Risk Assessment. *Journal of AHIMA, 84*(9), 66-70.

AHIMA (2018). About AHIMA. Retrieved on September 22, 2018 from http://www.ahima.org/about/aboutahima.

AHIMA Privacy and Security Council (2015). Sample (Chief) Privacy Officer Job Description. *AHIMA Body of Knowledge.* Retrieved on September 23, 2018 from http://bok.ahima.org/doc?oid=107672#.W6fZmGhKgdU

Amori, G. (2008). Preventing and responding to medical identity theft. *Journal of Healthcare Risk Management: The Journal of the American Society for Healthcare Risk Management, 28*(2), 33-42.

Andoh-Baidoo, F. K., Amoako-Gyampah, K., & Osei-Bryson, K. (2010). How Internet Security Breaches Harm Market Value. *IEEE Security & Privacy* (1), 36.

Andoh-Baidoo, F. K., & Osei-Bryson, K. (2007). Exploring the characteristics of Internet security breaches that impact the market value of breached firms. *Expert Systems with Applications,* 32703-725

Arrow, K. J. (1971). *Essays in the theory of risk-bearing* (Vol. 2). Amsterdam, London: North-Holland Publishing Company.

Babbie, E. R. (2001). *The practice of social research.* Belmont, CA: Wadsworth Cengage Learning.

Bai G, Jiang J, & Flasher R. (2017) Hospital Risk of Data Breaches. *JAMA Internal Medicine.* Ipswich, MA.

Bazerman, M. H. (1984). The Relevance of Kahneman and Tversky's Concept of Framing to Organizational Behavior. *Journal of Management, 10*(3), 333-343.

Bendix, J. (2013). What the HIPAA omnibus rule means for your practice. *Contemporary OB/GYN, 58*(6), 34

Bernoulli, D. "Specimen Theorise Novae de Mensura Sortis," Commentarii Academiae Scinetiarum Imperialis Petropolitanae Tomus V [Papers of the Imperial Academy of Sciences in Petersburg, Vol. V] 1738, p175-192 *Translated by Sommer, L., "Exposition of a New Theory on the Measurement of Risk." Econometrica, Vol 22, No 1 (Jan 54) p23-36*

Blanke, S. J., & McGrady, E. (2016). When it comes to securing patient health information from breaches, your best medicine is a dose of prevention: A cybersecurity risk assessment checklist. *Journal of Healthcare Risk Management, (1),* 14.

Blustein, A. & Lapidus, B. (2010). When do you notify after a HIPAA breach? *Same-Day Surgery, 34*(11), 129-131.

Boerner, C. M. (2010). View HIPAA breaches affecting 500 or more individuals online. *Journal of Health Care Compliance, 12*(3), 31-68.

Briggs, R. & Zalta, E. (2015). Normative theories of rational choice: Expected utility. *The Stanford Encyclopedia of Philosophy*. Retrieved from http://plato.stanford.edu/archives/win2015/entries/rationality-normative-utility/

Buffone, P. N. (2016). The 'Cure'-All for 21st Century Data Sharing. *Pharmaceutical Executive, 36*(8), 39.

California Office of Statewide Health Planning and Development (OSHPD) (2015). HIPAA Definitions and 18 Identifiers. Retrieved on March 6, 2015 from http://www.oshpd.ca.gov/Boards/CPHS/HIPAAIdentifiers.pdf

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security, 11*(3), 431.

Coate, D., & MacDonald, K. (2002). Projecting the budget impacts of HIPAA. *Healthcare Financial Management, 56*(2), 42-48.

Collins, J. D. W. (2007). Toothless HIPAA: Searching for a private right of action to remedy privacy rule violations. *Vanderbilt Law Review, 60*(1), 199-233.

Corbin, J, & Strauss, A. (2014). *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory.* Los Angeles, CA: SAGE Publications, Inc.

Dezenhall, E. (2015). A look back at the Target breach. Huffington Post. Retrieved on March 6, 2015 from http://www.huffingtonpost.com/eric-dezenhall/a-look-back-at-the-target_b_7000816.html

Dimick C. (2010) No harm done? Assessing risk of harm under the federal breach notification rule. *Journal of AHIMA. 81*(8):20-25

Eisenmann, C. (2009). When hackers turn to blackmail. *Harvard Business Review, 87*(10), 39-48.

Erlich, Y., Shor, T., Carmi, S., & Pe'er I. (2018). Re-identification of genomic data using long range familiar searches. *bioRxiv.* doi: https://doi.org/10.1101/350231

Evangeli, M., Kafaar, Z., Kagee, A., Swartz, L., & Bullemor-Day, P. (n.d). Does message framing predict willingness to participate in a hypothetical HIV vaccine trial: An application of Prospect Theory. *Aids Care-Psychological and Socio-Medical Aspects of Aids/Hiv, 25*(7), 910-914.

Federal Trade Commission, Bureau of Consumer Protection, Division of Consumer and Business Education. (2010). Medical identity theft. Retrieved June 6, 2017 from www.bcbsil.com/pdf/education/wellness/medical_id_theft_consumer_brochure.pdf

Fleming, N., Culler, S., McCorkle, R., Becker, E., Ballard, D. (2011). The financial and nonfinancial costs of implementing electronic health records in primary care practices. *Health Affairs 30*(3). 481-489.

Frank, J. (2016). Don't expect legislative defenses against cyberattacks anytime soon. *Medical Economics, (7),* 49.

Gabriel, M., Noblin, A., Rutherford, A., Walden, A., & Cortelyou-Ward, K. (2018). Data Breach Locations, Types, and Associated Characteristics Among US Hospitals. *American Journal of Managed Care, 24*(2), 78-84.

Gogtay, N. J. (2010). Principles of sample size calculation. *Indian journal of ophthalmology, 58*(6), 517.

Grando, M. A., Murcko, A., Mahankali, S., Saks, M., Zent, M., Chern, D., & Hassanzadeh, N. (2017). A Study to Elicit Behavioral Health Patients' and Providers' Opinions on Health Records Consent. *Journal of Law, Medicine & Ethics, 45*(2), 238-259.

Greene, T. (2015). Anthem hack: Personal data stolen sells for 10X price of stolen credit card numbers. *Network World.*

Hazra, A., & Gogtay, N. (2016). Biostatistics Series Module 4: Comparing Groups – Categorical Variables. *Indian Journal of Dermatology. 61*(4), 385-392.

Heubusch, K. (2011). Little Breaches: OCR Releases First "Small Breach" Data. *Journal of AHIMA, 82*(10), 56-57.

Holloway, M., & Fensholt, E. (2013). HHS finalizes HIPAA privacy and data security rules, including stricter rules for breaches of unsecured PHI. *Benefits Law Journal, 26*(2), 95-102.

Holmes, R., Bromiley, P., Devers, C. E., Holcomb, T. R., & McGuire, J. B. (2011). Management Theory Applications of Prospect Theory: Accomplishments, Challenges, and Opportunities. *Journal of Management,* 37(4), 1069-1107.

Hudson, K. L., & Collins, F. S. (2017). The 21st Century Cures Act - A View from the NIH. *New England Journal of Medicine, 376*(2), 111.

Jaccard, J., & Jacoby, J. (2010). *Theory construction and model-building skills: a practical guide for social scientists.* New York: Guilford Press,

Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision under risk. *Econometrica: Journal of the Econometric Society, 47*(2), 263-291.

Keeve, A. (2016). 7 PR lessons from the largest healthcare data breach in history. Retrieved on September 23, 2018 from https://www.prnewsonline.com/7-pr-lessons-from-the-largest-healthcare-data-breach-in-history/

Kerr, P., DeAngelis, D., & Brown, T. A. (2014). Five questions to ask before a data breach occurs. *Journal of Health Care Compliance, 16*(6), 27-71.

Khansa, L., Cook, D., James, T. & Bruyaka, O. (2012). Impact of HIPAA Provisions on the Stock Market Value of Healthcare Institutions, and Information Security and Other Information Technology Firms. *Computers & Security, 31*(6). 750-770.

Khansa, L., & Liginlal, D. (2009). Quantifying the Benefits of Investing in Information Security. *Communications of the ACM, 52*(11), 113-117.

Kim, K., Browe, D., Logan, H., Holm, R., Hack, L., & Ohno-Machado, L. (2014). Data governance requirements for distributed clinical research networks: triangulating perspectives of diverse stakeholders. *Journal of the American Medical Informatics Association, 21*(4), 714-719.

Korolov, M. (2015). Health-related data breaches could be expensive and life-threatening. *Network World.*

Kraemer, S., & Carayon, P. (2007). Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. *Applied Ergonomics, 38,* 143-154.

Kroll Advisory Solutions (2012). 2012 HIMSS analytics report: security of patient data. Retrieved on June 4, 2017 from http://csbweb01.uncw.edu/people/cummingsj/classes/mis534/articles/Previous%20Articles/Ch6SecurityReport.pdf

Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology & Health Care, 25*(1), 1-10.

LaTour, K. & Eichenwald-Maki, S. (2006). *Health Information Management Concepts, Principles, and Practice.* Chicago, IL: American Health Information Management Association.

LaTour, K. & Eichenwald-Maki, S. (2013). *Health Information Management Concepts, Principles, and Practice: Fourth Edition.* Chicago, IL: American Health Information Management Association.

Liginlal, D., Sim, I., & Khansa, L. (2009). How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. *Computers & Security, 28*215-228

Liginlal, D., Sim, I., Khansa, L., & Fearn, P. (2012). HIPAA Privacy Rule Compliance: An Interpretive Study Using Norman's Action Theory. *Computers & Security, 31*(2). 206-220.

Majumder, M. A., Guerrini, C. J., Bollinger, J. M., McGuire, A. L., & Cook-Deegan, R. (2017). Sharing data under the 21st Century Cures Act. *Genetics in Medicine, 19*(12), 1289-1294.

Marshall, A. (1890). Principles of economics: an introductory volume.

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data Privacy: Effects on Customer and Firm Performance. *Journal Of Marketing, 81*(1), 36-58.

McMillan, M. (2015). The cost of IT security. *Healthcare Financial Management: Journal of the Healthcare Financial Management Association, 69*(4), 44-47.

Melnik, T. (2012). Class actions, federal actions, and state actions: The data breach saga continues. *Journal of Health Care Compliance, 14*(2), 45-48.

Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Health and Human Services, 78 Fed Reg. (January 25, 2013) (to be codified at 45 C.F.R pts 160 & 164).

Novemsky, N. (2013). *Nathan Novemsky: Risk Aversion in Decision Making.* Retrieved from http://www.youtube.com/watch?v=9AXLmjoaI60&list=PLE7C7B02ACB9E746C&feature=share&index=5

Qniemiec (2011). *Risk Premium.* Used under CCO 1.0/Combined graphs. Retrieved from http://en.wikipedia.org/wiki/Risk_aversion

Parks, C., & Monson, K. (2017). Automated Facial Recognition of Computed Tomography-Derived Facial Images: Patient Privacy Implications. *Journal of Digital Imaging, 30*(2), 204-214.

Pallant, J. (2013). *SPSS survival manual: a step by step guide to data analysis using IBM SPSS.* Maidenhead, Berkshire, England: McGraw Hill.

Ponemon Institute (2013). Third annual patient privacy & data security study. Retrieved on June 4, 2017 from http://www.ponemon.org/library/third-annual-patient-privacy-data-security-study?s=privacy

Ponemon Institute (2014). Fourth annual benchmark study on patient privacy & data security. Retrieved on June 4, 2017 from http://www.ponemon.org/library/fourth-annual-benchmark-study-on-patient-privacy-data-security?s=privacy

Ponemon Institute (2015). Fifth annual benchmark study on patient privacy & data security. Retrieved on June 4, 2017 from http://www.ponemon.org/library/fifth-annual-benchmark-study-on-privacy-security-of-healthcare-data?s=privacy

Ponemon Institute (2016). Sixth annual benchmark study on patient privacy & data security. Retrieved on June 4, 2017 from http://www.ponemon.org/library/sixth-annual-benchmark-study-on-privacy-security-of-healthcare-data-1?s=privacy

Pratt, J. W. (1964). Risk aversion in the small and in the large. *Econometrica: Journal of the Econometric Society*, 122-136.

Pritts, J. (2002). Altered states: state health privacy laws and the impact of the federal health privacy rule. *Yale Journal of Health Policy, Law, and Ethics. 2*(2), 6.

Raosoft (2017). Sample size calculator. Retrieved June 6, 2017 from http://www.raosoft.com/samplesize.html

RAVE Mobile Safety (2018). Rave mobile safety survey unearths discrepancies about which emergencies occur at facilities and the preparedness plans they have in place. Retrieved

on November 4, 2018 from https://www.prnewswire.com/news-releases/rave-mobile-safety-survey-unearths-discrepancies-about-which-emergencies-occur-in-healthcare-facilities-and-the-preparedness-plans-they-have-in-place-300735983.html

Reinhart-Thompson (2013). *Introduction to Health Information Privacy and Security.* Chicago; Illinois: American Health Information Management Association, 2013.

Rothstein, M. (2013). HIPAA Privacy Rule 2.0. *Journal of Law, Medicine & Ethics, 41*(2), 525-528.

Salamon, L. M. (2002). *The tools of government: a guide to the new governance*. Oxford; New York: Oxford University Press, 2002.

Smith, K.B. & Larimer, C. W. (2013). *The public policy theory primer (*2nd ed.). Boulder, CO: Westview Press.

Squires, D. and Anderson, C. (2015). U.S. health care from a global perspective: spending, use of services, prices, and health in 13 countries. *The Commonwealth Fund, 1819* (15).

Terry, K. (2015). HIPAA breach: secure data & prevent fines--here's how. *Medical Economics, (14),* 26.

Tversky, A., & Kahneman, D. (1991). Loss aversion in riskless choice: a reference-dependent model. *Quarterly Journal of Economics, 106*(4), 1039-1061.

Tversky, A., & Kahneman, D. (1992). Advances in prospect theory: Cumulative representation of uncertainty. *Journal of Risk and uncertainty, 5*(4), 297-323.

United States. Department of Health and Human Services. Office for Civil Rights. (2011a). *Annual Report to Congress on Breaches of Unsecured Protected Health Information for Calendar Years 2009 and 2010.* Retrieved 9 November 2013 from the Department of

Health and Human Services website at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachrept.pdf

United States. Department of Health and Human Services. Office for Civil Rights. (2011x). *Annual Report to Congress on Breaches of Unsecured Protected Health Information for Calendar Years 2013 and 2014.* Retrieved 4 June 2017 from the Department of Health and Human Services website at https://www.hhs.gov/sites/default/files/rtc-breach-20132014.pdf

United States. Department of Health and Human Services. Office for Civil Rights. (2011b). *HHS Announces First HIPAA Breach Settlement Involving Less Than 500 Patients.* Retrieved 9 November 2013 from the Department of Health and Human Services website at http://www.hhs.gov/news/press/2013pres/01/20130102a.html

United States. Department of Health and Human Services. Office for Civil Rights. (2016). *FACT SHEET: Ransomware and HIPAA*. Retrieved 19 March 2017 from the Department of Health and Human Services website at https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf

United States. Department of Health and Human Services. Office for Civil Rights. (2017). *Resolution Agreements.* Retrieved 10 August 2010 from the Department of Health and Human Services website at https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html

United States. Government Accountability Office. (2016). Electronic *Health Information: HHS Needs to Strengthen Security and Privacy Guidance and Oversight.* Retrieved 10 August 2017 from https://www.gao.gov/products/GAO-16-771

Vinson, D. D. (2011). No more paper tiger: promise and peril as HIPAA goes HITECH. *Journal of Healthcare Risk Management, 30*(3), 28-37.

Warner, D. (2013). When to Send a Breach Notification: New HIPAA Rules Revise "Harm" Standard. *Journal of AHIMA, 84*(4), 42-43.

Wikina, S. B. (2014). What Caused the Breach? An Examination of Use of Information Technology and Health Data Breaches. *Perspectives in Health Information Management*, 1-16.

Wilder, M., Bennett, B., Bianchi, M., & Peters, N. (2013). HHS issues new HITECH/HIPAA rule: Top 10 changes. *Intellectual Property & Technology Law Journal*, *25*(5), 19-23.

Winn, P. A. (2001). Confidentiality in cyberspace: the HIPAA privacy rules and the common law. *Rutgers LJ*, 33, 617.

Wood, C. C., & Banks, W. J. (1993). Human error: an overlooked but significant information security problem. *Computers & Security,* (1). 51.

Zarate, O. A., Brody, J. G., Brown, P., Ramirez-Andreotta, M. D., Perovich, L., & Matz, J. (2016). Balancing Benefits and Risks of Immortal Data. *Hastings Center Report, 46*(1), 36-45.