A Framework for Evaluation of Risk Management Models for HIPAA Compliance for Electronic Personal Health Information used by Small and Medium Businesses using Cloud Technologies

by

Raymond Brett Luna

July 2018

Director of Thesis: Charles J. Lesko, Ph.D.

Major Department: Technology Systems

Our societal quest for collaboration and openness has always been in direct conflict with our desire to maintain our personal privacy. Those conflicting goals are more prominent than ever for healthcare, due to its rapid *Digital Transformation* and coupled with risk related to the exploitation of *Protected Health Information (PHI)* that is processed on cloud-based technologies by healthcare *Small and Midsize Businesses (SMB)*. Healthcare SMBs are at higher risk because they often have limited resources to identify and assess risk. This study focused on this issue through an exploratory inquiry using survey statistics, scholarly research, regulatory requirements, and best practices to develop a framework that can be used by healthcare SMBs to evaluate and select a risk assessment model. As illustrated in this study, the selected model can be leveraged to identify and assess risk associated with PHI that is processed in the cloud. This study included four key phases: confirmation of risk for PHI in the cloud, an investigation of HIPAA requirements and best practices for risk assessment, an evaluation of risk assessment models, and a risk assessment model selection process. As a result, healthcare SMB entities with limited resources can improve their ability to achieve HIPAA compliance through risk assessment and contribute to improvements for the overall patient care experience.

A Framework for Evaluation of Risk Management Models for HIPAA Compliance for Electronic Personal Health Information used by Small and Medium Businesses using Cloud Technologies

A Thesis

Presented to the Faculty of the Department of Technology Systems

East Carolina University

In Partial Fulfillment of the Requirements for the Degree

Master of Science in Network Technology: Information Security Concentration

by

Raymond Brett Luna

July 2018

A Framework for Evaluation of Risk Management Models for HIPAA Compliance for Electronic Personal Health Information used by Small and Medium Businesses using Cloud Technologies

by

Raymond Brett Luna

APPROVED BY:

DIRECTOR OF
THESIS:_____
Charles J. Lesko, Ph.D.

COMMITTEE MEMBER: _____
Philip J. Lunsford, Ph.D.

COMMITTEE MEMBER: _____
John L. Pickard, Ph.D.

CHAIR OF THE DEPARTMENT
OF TECHNOLOGY SYSTEMS: _____
Tijjani Mohammed, Ph.D.

DEAN OF THE
GRADUATE SCHOOL: _____
Paul J. Gemperline, PhD

ACKNOWLEDGEMENTS

Thanks first and foremost to my Lord and Savior who has blessed me with this incredible opportunity and the perseverance and skill required to complete this study and degree. I would also like to thank my immediate family for their undaunted support throughout this process, without whom I would have not been able to reach my goals towards completion of this degree while also balancing a busy career.

There are many people who have supported me throughout my educational and career endeavors, but I would specifically like to thank and acknowledge those few that directly helped to shape and support my learning experiences and career goals. The first are previous mentors who opened and guided important career opportunities for me; both in the U.S. Marine Corp and in various Information Technology leadership roles across numerous industries, including U.S. healthcare. I am also thankful for my thesis committee chair Dr. Charles J. Lesko and other committee members, Dr. Philip J. Lunsford and Dr. John L. Pickard for their combined guidance on helping me push forward to completion of this degree.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1. INTRODUCTION

Introduction to the Problem

Over the past decade, the significance of computers as key enablers for achieving both strategic and tactical business objectives have dramatically increased at an accelerated pace. As the world continues to undergo a *digital transformation*, several ongoing Information Technology (IT) trends supporting that transformation have been noted, including the Internet of Things (IoT), Predictive Analytics, and Artificial Intelligence (Newman, 2017). The difference between recent and future IoT trends will be the dynamic and interactive convergence of IoT capabilities. For example, IoT will move from its initial disparate deployment of smart devices to leveraging those devices across the Internet in highly integrated and automated ways.

On an industrial level, IoT already includes such digitized capabilities as controlling utility resource allocation and consumption, the automation of entire supply chains, and self-driving vehicles. These capabilities have created an explosion of continuous IoT growth that the world has not previously seen. As indicated in Figure 1, Cisco Systems projected that the number of connected IoT devices will exceed 50 billion by 2020 (Afshar, 2017), a more than 100% increase from 2016. This prediction reflects the growth rate of technology expressed by Moore's Law and is based on the industry assumption that there was an inflection point near the year 2009, which is believed to mark the inception of IoT, when the number of devices on the Internet first equaled the global population (Afshar, 2017).

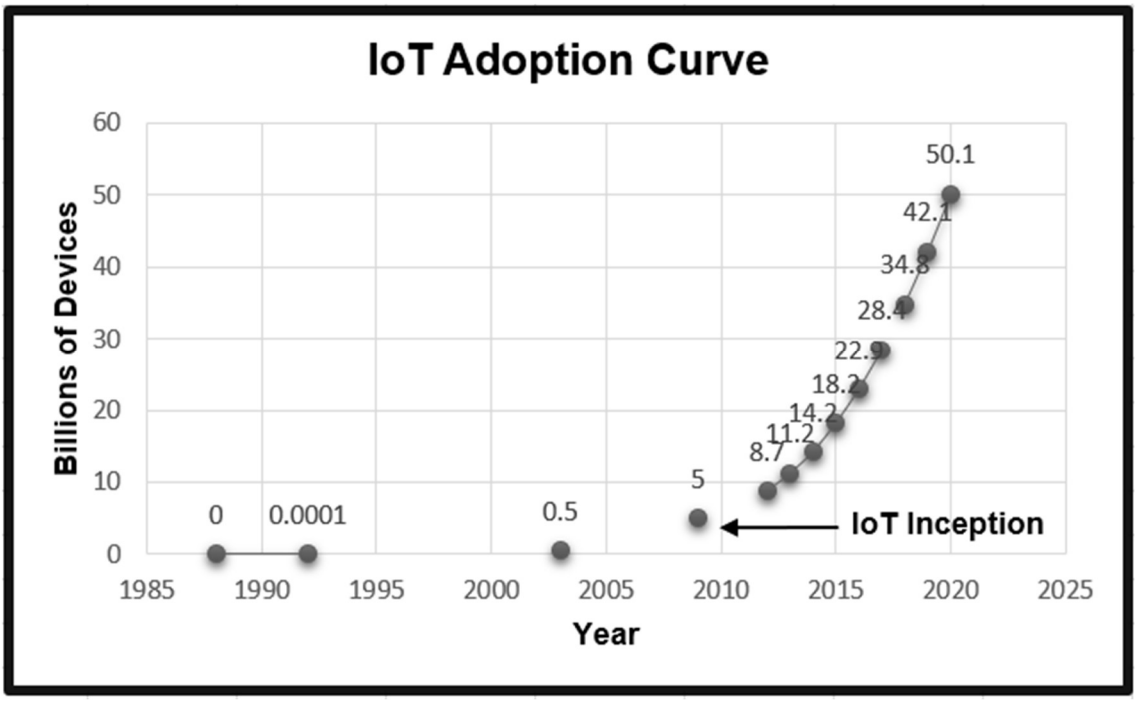

Figure 1. IoT growth projections from Cisco Systems (Afshar, 2017; Cisco, 2013).

Since Cisco first made this prediction in 2013, other industry leaders—such as Gartner, Hewlett-Packard and International Data Corporation (ICD)—have published more conservative predictions that put IoT growth at 20-30 billion devices by 2020 (Gartner, Inc., 2015; IDC, 2017). To comprehend Cisco's more extreme prediction of 50 billion devices, the purpose of this study, first, was to provide an understanding of the assumptions upon which this growth scenario is based. Cisco and other industry experts have been clear that the actual number of devices on IoT by 2020 will be dependent upon some basic assumptions about usage patterns on the Internet going forward. Several IoT industry experts have clearly articulated these assumptions. For example, Patterson (2017) explained that Internet infrastructure must be able to keep pace with device growth for Cisco's prediction to come to fruition. Patterson (2017)

further explained that IoT privacy and energy consumption issues would cause Cisco's prediction to fall short.

Maciej Kranz, Vice President of Strategic Innovation at Cisco Systems and a world-recognized expert on IoT, has elaborated on the catalysts that must be in place to drive extreme IoT growth predictions. In his Cisco blog, Kranz (2018) explained the necessary ingredients and conditions required to facilitate extreme IoT growth as follows:

- *Artificial Intelligence (AI)* – AI and machine learning (ML) will enable predictive analysis of real-time IoT data streams to drive more powerful decision making and AI will facilitate much faster IoT device onboarding.
- *Fog or Edge Computing* – In order for extreme IoT growth to be successful, real time data processing must occur on the "edge" of the network. Fog or edge computing is making that possible by scaling cloud computing to the consumer's network edge.
- *Blockchain* will provide secure, audit-level tracking of IoT data transactions, eliminating the need for a central, trusted intermediary between communicating devices. This is a basic requirement for highly regulated industries such as healthcare and finance (Krantz, 2018).

The capabilities that Kranz described (2018) are clearly at the forefront of industry discussion, proof of concept, innovation, and product development. Given the focus on, and investment levels in, these capabilities, the assumption behind this study was that the prerequisites required to support extreme IoT growth were underway and that they supported the midpoint-to-higher end of the IoT growth prediction range. Regardless of the final IoT count at the end of 2020, IoT growth is exploding, and it is not likely to slow down over the next several years. While this

rapid IoT growth is creating a hotbed for innovation, it is also presenting growing challenges for the protection of digital information.

The vulnerability challenges that the world is facing on the Internet are not related to IoT growth alone. More importantly, many "smart" devices on IoT are vulnerable, often because their platform footprint is too small to facilitate protective capabilities, or their default username and password is not changed at deployment (Symantec Security Response, 2016, pp. 1-2). Those vulnerabilities are further exacerbated by product marketing organizations that push devices to the IoT market before device security can be considered. Cybersecurity experts have been warning consumers over the past few years that hackers integrated into a network of bots that can execute denial of service attacks will compromise vulnerable IoT devices. In 2016, the Mirai malware attack was one large body of evidence that this prediction had come to fruition. On the heels of the Mirai attack, consumers were left asking what the probability is that a smart device on IoT will be attacked. Cyber security company Symantec Corporation responded with an analysis concluding that most IoT devices are scanned by various cybercriminals approximately every two minutes. This means that an unprotected IoT device, such as one with a default password, could be breached within minutes of going online (Symantec Security Response, 2016).

To further investigate and validate this research area, this study also considered theories about worldwide vulnerability rates. A team of scholars from The University of Arizona studied an array of IoT device types to infer their vulnerability rates and the scale of worldwide vulnerabilities overall. The vulnerability rates that they calculated included a broad variation that ranged from a low of 0.44% to a high of 40%, but the UA scholars argued that, given the number of devices on the Internet at that time (approximately 12 billion in 2014), "even the

lowest vulnerability rate of 0.44% would result in 4400 vulnerable systems for every million deployed" (Patton et al., 2014, pp. 4-6).

Given the dramatic growth of vulnerable devices and data on the Internet, the information processed by all those devices has become and will continue to be widely varied in scope and to include massive amounts of proprietary information and personal data that must be protected. Individual Internet users are sharing virtually all their personal information: from complete financial portfolios and tax information to their full medical histories. The diversity, distribution, value, and vulnerabilities that are characteristic of private personal information make it a prime target for exploitation by cybercriminals. Ponemon Institute, a well-known U.S. research firm that is often quoted by major news agencies as a credible source, is dedicated to advancing responsible information and privacy management practices in business and government. To achieve this objective, the Institute conducts independent research, educates leaders from the private and public sectors, and verifies the privacy and data protection practices of organizations in a variety of industries. Ponemon (2016) determined that since 2013, there has been a global increase of 29% in the total cost of data breaches. The United States was the biggest contributor to this statistic, with a 9% increase ranging from $201 million spent in 2014 to $221 million in 2016. In their study, Ponemon (2016) noted that a *data breach* is a compromised record that includes information that identifies the natural person (individual) whose information has been lost or stolen.

As depicted in Figure 2, the researchers who conducted the Ponemon study considered many factors of data breaches. For example, the biggest global financial consequence of data breaches is lost business. The U.S. led all other 383 companies surveyed across 12 countries by

an astounding 49%, paying the highest price, $3.97 million per incident, for lost business resulting from data breaches. This figure was 50% higher than the next highest country.

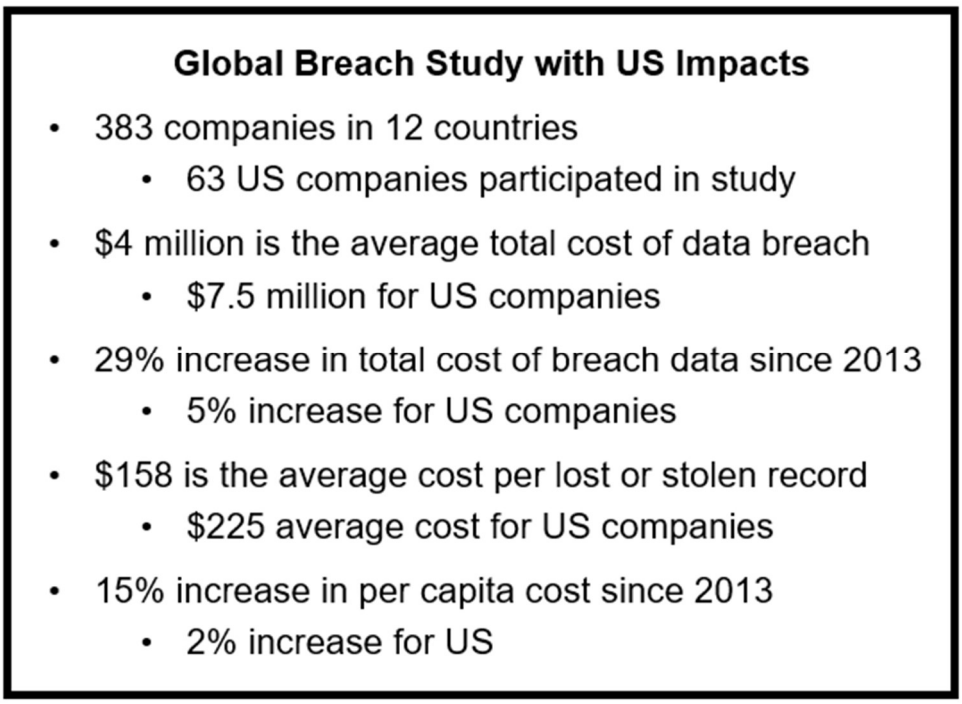

Figure 2. Ponemon Institute's global breach study highlights for 2016.

In addition to increases in the cost of data breaches, a later Ponemon (2018) study found, between 2016 and 2018 there was a 26% probability of a material data breach involving 10,000 lost or stolen records. While data breaches caused by system glitches and human error were considered and found to be higher than expected, the primary cause of these breaches was malicious or criminal attacks, at 48% globally, with 52% of those global companies being U.S. owned.

Because they are highly regulated, the healthcare and financial industries incur the highest indirect costs of data breaches in the U.S. Within the U.S. Healthcare industry, many different organizations provide an array of services that require access to personal health information and that are impacted by direct and indirect costs associated with data breaches. Cost

increase factors related to data breaches more specific to U.S. healthcare organizations include proactive management of *churn rate*, notification to breach victims, and the time it takes to identify and contain a breach. Churn rate is directly related to corporate campaigns that have a goal of reducing lost business by maintaining customer loyalty before a data breach occurs (Ponemon Institute, LLC, 2016). These cost factors contribute to what is known as indirect costs, and these indirect costs have increased in the U.S. roughly 60% over the past 12 years.

Background of the Study

Healthcare-related personal information is at the core of all healthcare IT systems. This information is also referred to as Protected Health Information (PHI). The U.S. Health Insurance Portability and Accountability Act of 1996 ("HIPAA") defines PHI as demographic information, medical history, test and laboratory results, insurance information, and other data that a healthcare provider uses to identify a patient and determine appropriate care. PHI has been protected by law since the inception of HIPAA in 1996 (DHHS Office for Civil Rights, 2013). For this study, all the PHI transactions considered are electronic; therefore, all PHI discussed is referred to as Electronic Protected Health Information (ePHI).

Systems that process ePHI transactions are spread throughout the healthcare ecosystem and are managed by a variety of stakeholders with varying degrees of discipline, capability, cost, and risk. This study focused on the stakeholders within the healthcare ecosystem that are specifically related to patient care, referred to as the patient care ecosystem. The patient care ecosystem is typically composed of one or more of the following: patients, healthcare providers, healthcare payers, pharmacy, business associates (includes ancillary service providers), and cybercriminals (Figure 3). *Healthcare stakeholders* who are in some way involved in patient

care and are, therefore, liable for compliance with HIPAA regulations are known as either *covered entities* or *business associates* that support these covered entities.

Covered entities include anyone contributing to the patient care lifecycle, including healthcare insurance companies (payers), doctors, hospitals, and pharmacies (providers).

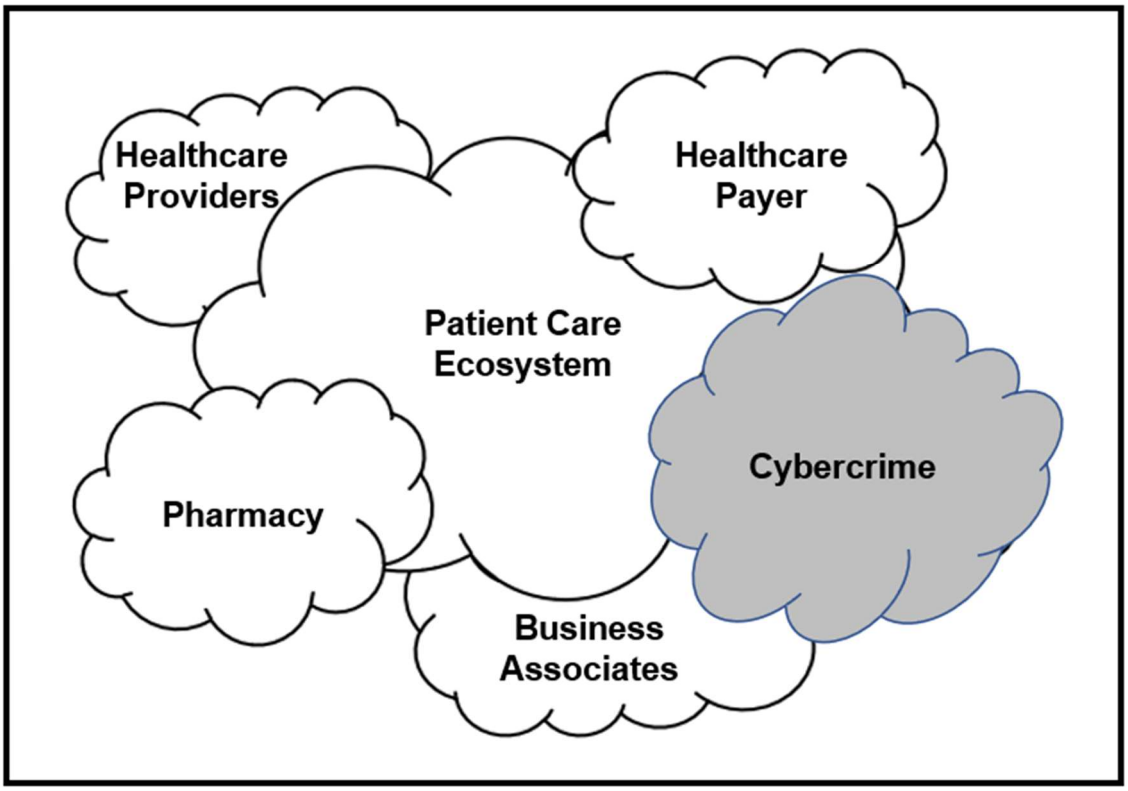

Figure 3. Patient care ecosystem: patients, covered entities (healthcare providers, payers, pharmacy), business associates and cybercriminals.

Business associates include those companies providing support for patient care, such as medical device companies, cloud providers, or any other organization or individual that performs services for a covered entity and has access to ePHI. While undesirable, cybercrime is also a key component of the patient care ecosystem. According to the U.S. Department of Homeland Security (2018), cybercrime is a crime carried out by means of one or more computers and a

network. For the purposes of this study, the scope of cybercrime was extended to include the Internet when it is used for processing ePHI to support patient care scenarios.

The combination of covered entities and business associates required to provide patient care varies broadly and depends upon a patient's specific medical issues and treatment. While payer organizations are typically large and have significant resources available to protect ePHI, they also tend to be the most risk averse. Small and Midsize Businesses (SMBs) run by private practice providers and their business associates, who are a variety of patient treatment delivery organizations (e.g., ancillary service providers such as medical device companies, transportation services, etc.) tend to have fewer resources with which to protect ePHI. Throughout this study, U.S. Healthcare Small and Midsized Business Covered Entities and Business Associates (SMBE&A) refer collectively to U.S. Healthcare Small and Midsized Business Covered Entities and Business Associates. SMBE&A further defines SMB to healthcare industry as related to HIPAA requirements for covered entities and business associates.

For several years, industry experts have valued ePHI records to be worth at least ten times more than a person's credit card information on the black market (Humer & Finkle, 2014, p. 1). Jackson (2014) substantiated this claim by stating,

> Stolen health credentials can go for $10 each, about 10 or 20 times the value of a U.S. credit card number, according to Don Jackson, Director of Threat Intelligence at PhishLabs, a cybercrime protection company. Mr. Jackson obtained the data by monitoring underground exchanges where hackers sell the information. (pp. 1-2)

ePHI has such a high bounty for cybercriminals because these data include patient names and their birthdates, insurance policy numbers, diagnostic codes, and medical billing information. Criminals have used this information primarily to submit fraudulent insurance claims.

The variety of patient data protection capabilities that exists between covered entities and business associates often makes for challenging business partnerships that can create additional risk as well as a more frustrating healthcare experience for patients. These variables, along with the mass movement of healthcare information to various cloud-based hosting and application deployment models and the desire to support full digitization of the healthcare ecosystem, make ePHI a prime target for cybercriminals. For example, according to healthcare IT security firm Redspin, over 100 million ePHI records have been stolen in a HIPAA data breach since 2009. These data breaches have taken place within numerous recognizable healthcare brands, such as Blue Cross Blue Shield of Tennessee (with 1 million victims), TRICARE Management Activity with (4.9 million victims), and the highly publicized breach in 2015 at Anthem with (80 million victims) (JA, 2015).

If larger healthcare companies with strong financial resources are at risk, it is not difficult to infer that healthcare SMB organizations are likely at even greater risk of being breached and their ePHI being compromised. Timothy Francis, an enterprise leader for the cyber insurance product line at Travelers Insurance, in a 2105 panel discussion, noted that although most cyber breach headlines are from larger corporate institutions, SMB breaches are far greater in number. The 2015 panel highlighted that 62% of cyber breach victims are SMB, further noting that most SMB preparation for breaches is low and that the costs of customer notification alone can be financially irreparable (Donlon, 2015).

To better understand the breadth and depth of this problem for SMB's, this study considered data from The U.S. Office of Advocacy of the Small Business Administration, which defines small business as independent companies that have 1-499 employees (Donlon, 2015). With a footprint of 99.7%, small businesses make up most U.S. businesses. If 62% of small

businesses are victims of cyber-breach, as Francis (cited in Donlon, 2015) suggest, given a criminal preference for healthcare patient data, this is a major problem for SMB healthcare companies, and further research into mitigation is firmly justified.

ePHI is deliberately targeted when it is hosted or processed on cloud-based assets. SMBE&A organizations are concerned most about ePHI data when it is in transit (as it moves from point-to-point across the Internet) and at rest (when digital copies of ePHI are hosted on various systems, storage, multi-tenant environments, etc.). Essentially, any ePHI being hosted or processed on IT assets that are not under the control of the SMBE&A is a concern for that population. With the goals of reducing stakeholder risk and improving patient confidence that their ePHI is being protected when managed by SMBE&A on the Internet and through cloud-based IT assets, this research study sought to address healthcare stakeholder concerns by discussing and offering *risk management* model options and best practices.

The researcher for this study has over 30 years of experience in the field of Information Technology, which includes 20 years in various healthcare IT roles, and, thus, is a key research instrument within this study. As Chief Information Officer at an SMB healthcare technology company that relies significantly on external integration with dozens of covered entities and business associates to process patient data across disparate cloud assets, the researcher brings a unique perspective and rich experience (Sulem, 2017, pp. 1-2).

Problem Statement

This study focused on the need to identify, assess, and reduce risk associated with the protection of ePHI while it is being processed in the cloud by SMBE&A, and to do so in a way that is HIPAA compliant. More specifically, this study sought to identify what research has been conducted and what solutions are currently being leveraged to identify and assess ePHI

vulnerabilities so that HIPAA compliance can be achieved. The healthcare scenario studied for this research effort was a simple patient care scenario (Figure 3) that leverages various cloud-based resources owned or operated by a variety of healthcare-covered entities and business associates. While larger healthcare payer and provider organizations tend to have an abundance of resources at their disposal, SMBE&A often do not. This makes these smaller healthcare organizations more susceptible to ePHI vulnerabilities.

Purpose of the Study

The purpose of this exploratory inquiry is to help SMBE&A to choose an appropriate *risk assessment* model that is low cost, easy to implement, and that can be used to determine the level of risk for ePHI as it is processed through cloud-based systems. This study contributes to that purpose by providing research on the following:

(1) Identification of the likelihood and impacts of risk associated with SMBE&A that process cloud-based ePHI transactions while participating in patient care (Figure 3). Then, using that information, considering best-fit risk assessment models and capabilities for the SMBE&A population.

(2) Discovery of shortfalls related to existing healthcare risk-centric research by addressing gaps that center around the evaluation and selection of risk assessment models and capabilities for SMBE&A.

(3) Research and added value for SMBE&A that have limited amounts of the resources required to select and leverage risk assessment capabilities to evaluate the risk levels associated with the ePHI that they process.

As a result, the SMBE&A population can increase its ability to achieve HIPAA compliance, remain in business by providing an appropriate level of protection for ePHI, and improve the overall patient care experience.

Research Questions

As described throughout this study's background, purpose, and literature review chapters, SMBs in the U.S. healthcare industry are at risk of HIPAA data (ePHI) breaches. Therefore, they require the ability to select and leverage an appropriate risk assessment model when ePHI is processed within cloud-based systems. To define and support the research required for this study, a research design that considered both qualitative and quantitative information was used. The areas of focus for this design are presented here as the research questions (RQ) that were used for this study:

RQ1: Does the risk of an ePHI breach justify the need to leverage a viable risk assessment model for the SMBE&A population?

RQ2: Through evaluation and assessment of HIPAA regulatory requirements and impacted IT architecture, what are the current *risk factors* for risk assessment that are critical for the SMBE&A population?

RQ3: Through evaluation and assessment of current risk models that meet HIPAA risk factor needs, what are candidate models for the SMBE&A population?

RQ4: What selection decision capability can be used by the SMBE&A population to evaluate and select an appropriate risk assessment model and how can the chosen model be leveraged to evaluate risk levels?

Method and Approach

This study proceeded in four key phases: (a) Confirmation of ePHI Breach Risk; (b) Decomposition of HIPAA Requirements for ePHI and Impacted Cloud-based Technology; (c) Evaluation of Risk Assessment Models; and (d) Risk Assessment Model Selection Process.

1. Phase One - Confirmation of ePHI Breach Risk: In phase one of the study, the background, problem, and purpose were researched and presented to confirm that ePHI is at risk when processed in the cloud. The finding of phase one was that further research is required for the SMBE&A population regarding the need to assess risk levels for ePHI being processed on cloud-based systems. In the initial part of phase one, risk impacts related to rapid IoT growth and related vulnerabilities were first considered. Phase one continued with qualitative research supported by surveys that assessed the impact on global companies from breaches of personal information. The research was then refined to focus specifically on ePHI breaches within the U.S. healthcare industry. The impact of ePHI breaches was then quantified with data retrieved from the U.S. Department of Health and Human Services' (DHHS) Office of Civil Rights (OCR) to validate the assumption that ePHI is truly at risk and that these breaches result in HIPAA violations, financial problems, and other negative outcomes for the impacted healthcare stakeholders.
2. Phase Two - Decomposition of HIPAA Requirements for ePHI and Impacted Cloud-based Technology: The second phase of this study began with a comprehensive decomposition of HIPAA requirements for ePHI to provide a clear picture for what constitutes an ePHI vulnerability that is out of compliance with HIPAA requirements. Next, the second phase applied HIPAA compliance requirements and risk

management best practices published by NIST to understanding HIPAA risk assessment requirements. Criteria were developed to evaluate various risk assessment and analysis models that can be leveraged to assign risk levels at various integration points across a given patient care scenario. For selecting the technical areas of high risk to be considered in the chosen risk assessment model, phase two concluded with a decomposition of the characteristics of *cloud computing* and a layered protective architecture model that helps create transparency in areas that are likely at high risk of SMBE&A breaches when ePHI transactions are processed in the cloud.

3. Phase Three - Evaluation of Risk Assessment Models: Phase three used the HIPAA, NIST, and NSA Defense in Depth (DiD) requirements identified in phase two to develop *risk analysis* and management steps based on key risk factors that were considered to create selection criteria for the risk assessment models. Phase three concluded with research on three different risk assessment methodologies that included probable alignment with the defined selection criteria.
4. Phase Four - Risk Assessment Model Selection Process: Phase four first considered research on selection decision models and processes that can be used to support the process of selection for risk assessment models applied to the SMBE&A population. After the selection of a decision matrix model, phase four then applied the selection criteria defined in phases two and three to the chosen decision matrix model and used that populated model to evaluate and rate each of the risk assessment models identified in phase three. The risk assessment model evaluated with the highest rating was selected. Phase four concluded with a sample case for the chosen risk

assessment model that provided a practical example of how the chosen model can be used by the SMBE&A population. Gaps and future research opportunities were also identified and discussed.

Significance of the Study

For several years, security experts have warned that cybercriminals are increasingly targeting the $4 trillion (as of 2017) U.S. healthcare industry. The primary reason for this is that stolen ePHI can sell for $10 per record, approximately ten to twenty times the street value of a U.S. credit card number (Humer & Finkle, 2014). In their cost of data breaches study, the Ponemon Institute (2016) found that between 2016 and 2018, there was a 26% probability that at least 10,000 lost or stolen records would be involved in each material breach. In the U.S. healthcare industry, the largest fiscal impact from data breaches is associated with lost business: "The cost component of lost business includes the abnormal turnover of customers, increased customer acquisition activities, reputation losses, and diminished goodwill" (Ponemon Institute, LLC, 2016, pp. 5-6) as well as lost business related to HIPAA law enforcement and penalties.

Healthcare stakeholders impacted most by these losses are SMBE&A, as defined in HIPAA regulations. Stakeholders that contribute to patient care include broad variation in terms of their ability to mitigate risks associated with breaches of patient data. For example, payer organizations (healthcare insurance companies) are typically larger and have more resources available to protect ePHI than SMBs run by private practice providers (doctors, clinics, etc.) and their business associates, which include a variety of treatment delivery organizations (e.g., online discount pharmaceutical suppliers, medical device companies, etc.), tend to have fewer resources with which to protect electronic assets.

The significance of this study is that it directly contributes to the awareness and possible mitigation of risks associated with SMBE&A that are at high-risk of patient data breaches. The individuals and companies that can benefit most from this study include SMB healthcare organizations that contribute to patient care and process patient data and the patients being treated. Specifically, the first line of defense for healthcare stakeholders are companies' IT Security managers and professionals. This study helps to equip those teams and individuals with the ability to quickly, easily, and cost effectively evaluate and select a risk assessment model that assists them to identify and assess high-risk scenarios, including vulnerabilities that can be exploited by cybercriminals and result in a breach of ePHI. The benefits include the reduction of patient frustration, the reduction of costs to SMBE&A that result from data breaches, the reduction of overall healthcare costs, the reduction of overall healthcare stakeholder risk aversion, and the protection of patient data.

Assumptions and Limitations

The survey data researched, referenced, and used for this study provide strong evidence that ePHI has a high probability of data breach when processed by SMB healthcare stakeholders on cloud-based assets. While this study does include research around data breach as it pertains to the impacts of HIPAA compliance, it did not cover other data breach concerns, other industries, or the entire healthcare patient ecosystem, however. Rather, this study was specifically focused on simple patient care scenarios that involve an insurance company, a healthcare provider (a private practice for general family medicine), an online pharmacy delivery company, and associated technology providers.

The HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework was used in this study to help organizations in any industry to understand, communicate, and manage

cybersecurity risks in a way that is aligned with *HIPAA Security Rule* requirements. While the entire crosswalk table and its contents should be considered when planning a company's Enterprise Information Security Program and protective measures for the HIPAA Security Rule, this research study focused only on the crosswalk categories and subcategories (as listed at Table 1 and further refined at Table 5) that directly impact the privacy and integrity of patient information as it moves, across the Internet, through and between covered healthcare entities and their business associates.

The risk assessments conducted for the purposes of this study were limited to SMBE&A. The critical selection criteria for an appropriate risk assessment model were that the model should be easy to use, low cost, and include flexibility that aligns with HIPAA requirements. As a result, the target users for this study are SMB healthcare stakeholders that process ePHI with cloud-based systems and networks. Therefore, the scope for this study was limited to finding a framework that healthcare SMB organizations can leverage that includes selection criterion and a selection process for risk assessment models based on HIPAA compliance requirements.

Development of a comprehensive risk management plan and maintaining security measures were outside the scope of this study. Because this study is focused on the evaluation and selection of a risk assessment model and method, the implementation of risk mitigation solutions was also not considered in scope of this study. Other technology areas that were out of scope for this study included: data backup and recovery, high availability, disaster recovery, network traffic flow control, intrusion detection systems, data loss prevention, enclave boundary defense, API management, GDPR, and Blockchain. Technologies that are in scope and related to protection of data at-rest and in-transit, are in Chapter 2 at the section titled "Layered Protective Architecture: Defense in Depth Approach".

Definition of Terms

Artificial Intelligence (AI) – (a) A facet of computer science that addresses computers developed to simulate intelligent behavior (b) when intelligent human behavior can be emulated by a machine (Merriam-Webster, 2108).

Blockchain – Technology that leverages cryptocurrency to create and facilitate peer-to-peer payment and ledger capabilities that are considered highly secure from breach. Bitcoin and a blockchain ledger work together to create this capability (Pemberton-Levy, 2016).

Business Associates - Ancillary support for patient care, such as medical device companies or any other organization or individual that performs services for a covered entity and has access to ePHI (Office for Civil Rights [OCR], 2003).

Cloud Computing - Model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction (Mell & Grance, 2011).

Covered Entities - Specific HIPAA terminology, like "Healthcare Stakeholders," that includes anyone contributing to the patient care lifecycle, such as healthcare insurance companies (payers), doctors (providers), hospitals, and pharmacies (DHHS Office for Civil Rights, 2017).

Data Breach - Event in which an individual's name plus a medical record and/or a financial record or debit card is potentially put at risk, with a compromised record being defined as information that identifies the natural person (individual) whose information has been lost or stolen in the data breach (Ponemon Institute, LLC, 2016).

Defense in Depth (DiD) – The Information Assurance Department (IAD) of the National Security Agency (NSA) defines DiD as a practical strategy for achieving Information Assurance in today's highly networked environments. DiD strategy is dependent upon on the intelligent application of currently available techniques and technologies (National Security Agency, 2015).

Digital Transformation - Use of technology to radically improve the performance or reach of enterprises. Executives in all industries are using digital advances such as analytics, mobility, social media, and smart embedded devices, as well as improving their use of traditional technologies such as ERP, to change their customer relationships, internal processes, and value propositions (Westerman, Bonnet, & McAfee, 2014).

Electronic Data Exchange (EDI) – Computer-to-computer transfer of business transaction information using standard, industry-accepted message formats (EDI Basics, 2018).

Electronic Health Record (EHR) - Patient data associated with a specific individual (including PHI) that can span multiple healthcare providers (Robichau, 2014).

Electronic Medical Record (EMR) - System used by a healthcare provider to manage the care of patients (Robichau, 2014).

Explanation of Benefits (EOB) - Insurance companies' written explanations regarding a claim showing what they paid and what the patient must pay (HealthInsurance.org, 2018).

Electronic Protected Health Information (ePHI) - PHI that is in electronic format (Jones, 2014).

Fog Computing – Also known as "edge computing," fog computing extends the cloud to make it in closer proximity to devices and systems that create and act on IoT data. Fog nodes can be activated anywhere that there is a network connection. This is done to decrease the

performance latency that can be experienced with a typical cloud connection (Cisco Systems, Inc., 2015).

Healthcare Stakeholders - Entities that participate in the patient care lifecycle, including insurance companies (payers), doctors, hospitals, clinics, pharmacies, medical device companies, etc. (Robichau, 2014).

HIPAA - Health Insurance Portability and Accountability Act of 1996 ("HIPAA") was federal legislation designed to improve both the efficiency and effectiveness of the national healthcare system by standardizing electronic healthcare transactions and identifiers. It also established safeguards to protect patient privacy and to ensure that patient data were secured and treated with respect and confidentiality (Office for Civil Rights [OCR], 2003).

HIPAA Claim Payment Transaction (Claim Payment) - HIPAA EDI Transaction (835) used to make a payment, send an Explanation of Benefits (EOB) remittance advice, or make a payment and send EOB remittance advice only between a health insurer and a health care provider either directly or via a financial institution (EDI Basics, 2018).

HIPAA Claim Submit Transaction (Claim Submit) - HIPAA EDI Transaction Claim Submit (837) used to submit a health care claim billing information, encounter information, or both, except for retail pharmacy claims (see EDI Retail Pharmacy Claim Transaction). It can be sent from the providers of health care services to payers either directly or via intermediary billers and claims clearinghouses (EDI Basics, 2018).

HIPAA Eligibility Inquiry Transaction (Eligibility Inquiry) - HIPAA EDI Transaction (270) used to inquire about the health care benefits and eligibility associated with an insurance subscriber or subscriber dependent (EDI Basics, 2018).

HIPAA Eligibility Response Transaction (Eligibility Response) - HIPAA EDI Transaction (271) used to respond to an inquiry about the health care benefits and eligibility associated with an insurance subscriber or subscriber dependent (EDI Basics, 2018).

HIPAA EDI Transaction Standards - HIPAA EDI Transaction Standards, a key component of HIPAA, establish national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers (EDI Basics, 2018).

HIPAA Privacy Rule - Standards for the privacy of individually-identifiable health information ("Privacy Rule") that established a set of national standards for the protection of certain health information. The U.S. Department of Health and Human Services ("HHS") issued the Privacy Rule to implement the requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") (DHHS: Office for Civil Rights, 2013).

HIPAA Security Rule - Requires health care providers, health plans, and business associates to conduct risk analyses and implement technical, physical, and administrative safeguards for ePHI (Office of the National Coordinator for Health Information Technology [ONC], DHHS Office for Civil Rights [OCR], & DHHS Office of the General Counsel [OGC], 2017).

Internet of Things (IoT) - Intel defines the Internet of Things (IoT) as a "robust network of devices, all embedded with electronics, software, and sensors that enable them to exchange and analyze data" (Intel, Inc., 2016, p. 3). However, many scholars and industry experts argued, at an NIST-sponsored academic seminar, that any set definition of IoT would be too limiting in a rapidly evolving field. In the same NIST workshop proceedings, researchers agreed that IoT is "a means to connect purpose-built items that leverage communication sensors to bridge the physical world with the electronic one" (Megas, Piccarreta, & O'Rourke, 2017).

Protected Health Information (PHI) - Generally refers to demographic information, medical history, test and laboratory results, insurance information, and other data that a healthcare provider uses to identify a patient and determine appropriate care (Office for Civil Rights [OCR], 2003).

Risk Analysis - Synonymous with Risk Assessment (NIST: Joint Task Force for Transformation Inititative, 2012).

Risk Assessment - Component of Risk Management that identifies (a) threats to the organization or threats directed through organizations against other organizations or the Nation, (b) vulnerabilities internal and external to organizations, (c) the harm that may occur given the potential for threats exploiting vulnerabilities, and (d) the likelihood that harm will occur. The result is a determination of risk (level of risk and degree of harm) (NIST: Joint Task Force for Transformation Inititative, 2012).

Risk Factor - Characteristic used in a risk model as an input to determine the severity of risk in a risk assessment (NIST: Joint Task Force for Transformation Inititative, 2012).

Risk Management - Process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level (NIST: Joint Task Force for Transformation Inititative, 2012).

Small and Midsize Business (SMB) - In the context of IT, Gartner defines an SMB as a business that, due to its size, has different IT requirements—and often faces different IT challenges—than large enterprises and whose IT resources (usually budget and staff) are often highly constrained (Gartner, Inc., 2018).

Organization of Thesis

This study was designed to support the assertion that processing healthcare transactions that include ePHI on the Internet creates the risk of personal data becoming compromised and

exploited by cybercriminals. Research and findings on several subjects that support this assertion were revealed. For example, evidence was presented from research on Internet vulnerabilities and HIPAA compliance concerns that support the existence of ePHI risk levels when health care data are hosted in the cloud. This study defined criteria that were used to evaluate various risk assessment and analysis models that can be leveraged to assign risk levels at various integration points across a given patient care scenario. The chosen selection criteria were then used to evaluate and select a risk assessment model that aligns well with the needs of SMB healthcare companies that process ePHI in the cloud.

Chapter 2 describes existing scholarly and industry research related to this topic with the goal of determining what is known and is not known about the topic. Chapter 3 examines how the research questions were addressed and describes the research design approaches used for this study: a pragmatic point of view, a primarily qualitative design that includes quantified information and a data collection method and data analysis practices utilized to support the research questions presented in Chapter 1. In Chapter 4, the findings of the analysis and a summary of the results are presented. Finally, Chapter 5 contains an interpretation of the results from Chapter 4, the study's conclusions based on the findings, and a discussion of this research as well as recommendations for future research.

CHAPTER 2. LITERATURE REVIEW

Introduction

This literature review chapter illustrates how knowledge has been built up in the combined research fields of IoT and healthcare. It also examines HIPAA requirements, vulnerabilities associated with ePHI hosted in the cloud, risks associated with SMBE&A, risk assessment models that assist with identification and evaluation of vulnerabilities for ePHI, and selection criteria based on HIPAA requirements that can be used to select an appropriate risk assessment model and methodology. This research is intended for use by SMBE&A organizations that seek to identify and reduce risks associated with processing ePHI in the cloud. The research for this literature review addresses Research Areas (RA) 1-4 to provide data relevant to research questions (RQ) 1-4 defined in Chapter 1, as follows:

- RA1 – Research presented in chapters 1 and 2 regarding Internet growth and related vulnerabilities justifies the need to leverage an appropriate risk assessment model for SMBE&A.
- RA2 – Research presented in Chapter 2 regarding HIPAA regulatory requirements and enforcement, along with guidance from NIST and NSA (DiD), identifies related characteristics and risk factors later used in this study to evaluate, select, and utilize an appropriate risk assessment model for the SMBE&A population.
- RA3 – Research presented in Chapter 2 identifies and evaluates risk assessment models that are likely selection candidates for the SMBE&A population.
- RA4 – The research presented in Chapter 2 identifies an effective decision matrix process used in this study to evaluate and select a risk assessment model appropriate for the SMBE&A population.

By demonstrating the achievements but also the limitations of previous research, this chapter presents a justification for the research to be undertaken.

HIPAA and its Enforcement with Privacy Rule and HITECH

The protection of patient healthcare information has been a long-standing problem with many complex legal implications. In the United States, patient information is protected by the Health Insurance Portability and Accountability Act of 1996, also known as HIPAA. HIPAA was enacted by the U.S. Congress and signed by President Clinton with the goal of protecting patient privacy and helping to ensure insurance coverage for individuals with pre-existing conditions. Because of HIPAA, healthcare payers, providers, and business associates are required to ensure the privacy and confidentiality of all patients' medical and billing records.

To guide the enforcement of HIPAA, The U.S. Department of Health & Human Services (DHHS) (2013) implemented the HIPAA Privacy Rule, which states,

> The Privacy Rule standards address the use and disclosure of individuals' health information—called "protected health information" by organizations subject to the Privacy Rule—called "covered entities," as well as standards for individuals' privacy rights to understand and control how their health information is used.

A department within DHHS known as the Office for Civil Rights (OCR) has been assigned accountability for the enforcement of compliance and financial penalties for non-compliance with the Privacy Rule.

The costs of HIPAA violations include both civil and criminal violations and penalties. When a covered entity is found to be noncompliant with HIPAA and does not satisfactorily resolve the matter, OCR will decide whether to impose Civil Money Penalties (CMPs) on the covered entity (American Medical Association, 2018). Financial penalties associated with civil

cases range between $100-$50,000 per violation and a maximum of $1.5 million per year. Covered entities that commit criminal violations of HIPAA are addressed by the Department of Justice. As with HIPAA civil penalties, there are a variety of levels of severity for criminal violations for noncompliance (American Medical Association, 2018). Depending on the severity of the violation, criminal penalties can range from a $50,000 fine and one year of jail time to $250,000 fines and ten years of imprisonment.

Figure 4 illustrates the OCR HIPAA violation settlements that occurred in between the years 2015-2018; the overall downward trend in settlements for this period suggests that healthcare companies are taking corrective action before a financial penalty is imposed on them or a settlement is agreed to (Compliancy Group, 2018). This study also highlights the fact that if 2018 continues its current annual trend in settlements, the year would end at ~$27M in settlements, resulting in a shift back to an upward trend. The number of all HIPAA violation cases currently under investigation is much larger. A comprehensive report for all active investigations can be located on the OCR website at their "Breach Portal," also known as their "Wall of Shame" (DHHS Office for Civil Rights [OCR], 2018).

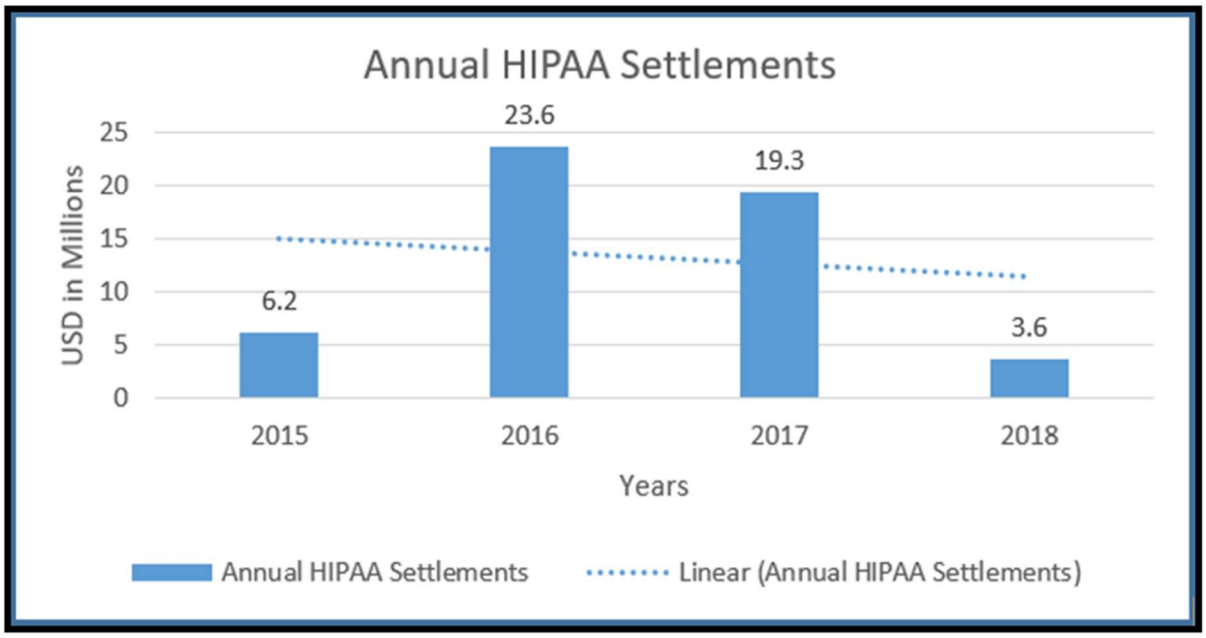

Figure 4. Annual HIPAA financial settlements.

The Breach Portal is highly interactive and, through a few search filters, quickly reveals evidence supporting the assertion that ePHI is at an elevated risk of a cyber-breach. For example, in 2017 alone, OCR investigated 123 covered entities or business associates for HIPAA violations. The total number of individuals potentially affected across all reported parties was 3.1 million. Figure 5 shows a distribution of affected individuals by breached IT asset. When compared with the data in Figure 4, most breach costs appear associated with corrective compliance actions taken to avoid financial penalties and to maintain a good reputation with customers.

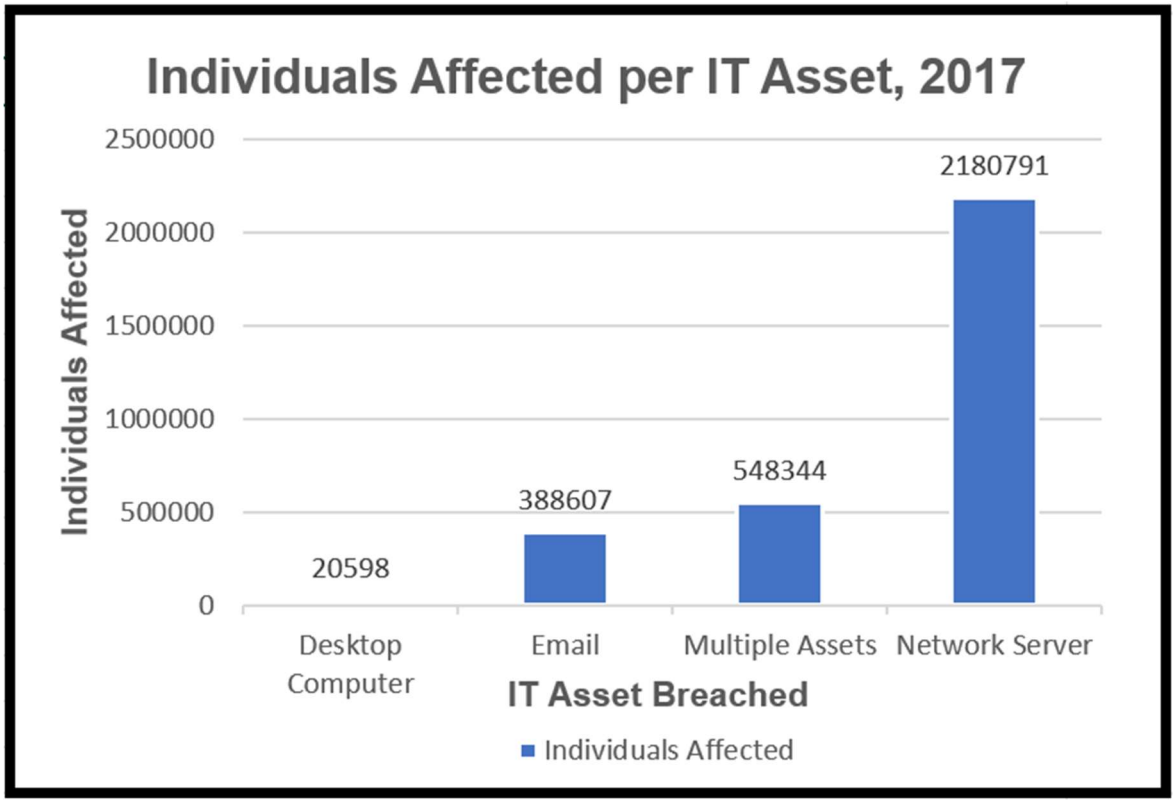

Figure 5. Breach cases under investigation by OCR, 2017.

Further, the 70% figure for individuals affected by breaches of ePHI resulted from vulnerabilities associated with network-based server infrastructures (DHHS Office for Civil Rights [OCR], 2018).

This study considered the cost of data breaches (as discussed in Chapter 1). Combined with the business impacts from data breaches in healthcare, that aggregate data revealed several keys points as described in Figure 6. The following themes emerge from these combined data sets:

- On a global level, the U.S. incurs the highest annual cost from data breaches compared to other countries.

- The U.S. healthcare industry is the largest contributor to the cost of data breaches in the U.S. Regulatory requirements and "cyber bounty" for ePHI are the key drivers of this cost.
- With 99% of U.S. companies being SMB, 62% of those SMBs being data breach victims in recent years, and 20% of those SMB breach victims being healthcare entities that contribute to the high number of U.S. citizens who have had their ePHI breached, there is serious cause for concern about ePHI becoming compromised.

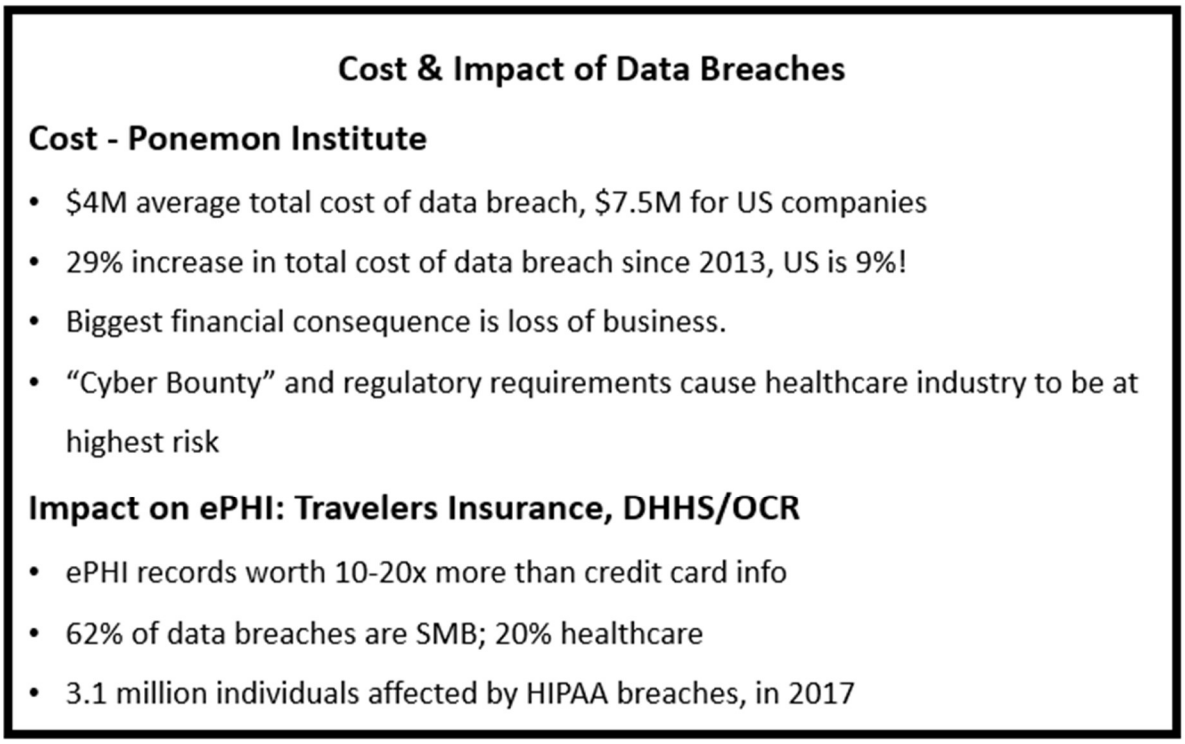

Figure 6. Summary of costs and impacts for data breaches.

A primary goal of the Privacy Rule is to ensure that ePHI is protected from compromise and, at the same time, allows for the continuous flow of patient health information required to promote patient care and wellness (DHHS: Office for Civil Rights, 2013). Healthcare stakeholders covered by the Privacy Rule include Health Insurance Plans (also known as "payers," or insurance companies that provide healthcare insurance products and services),

Health Care Providers (also known as "providers," or individuals and entities that provide care or treatment to patients), Health Care Clearinghouses (entities that process nonstandard information that they receive in a standard format from another entity), and various business associates that support the aforementioned covered entities. These healthcare stakeholders are all accountable for compliance with the Privacy Rule.

Patient information protected by the Privacy Rule is known as Protected Health Information (PHI). The Privacy Rule ensures that all individually identifiable health information is protected as it flows through and between healthcare stakeholders (i.e., covered entities and business associates). A simple example of this information flow can be illustrated with the transaction lifecycle of a patient who is prescribed medication by a provider: The prescription is processed and delivered by an online pharmacy and payment for it is processed by the patient's insurance company (payer). Key components of this transaction lifecycle are depicted in Figure 7 and include HIPAA Electronic Data Exchange (EDI) Transaction Standards, such as the following:

- Explanation of Benefits (EOB);
- HIPAA Claim Payment Transaction (Claim Payment / 835);
- HIPAA Claim Submit Transaction (Claim Submit / 837);
- HIPAA Eligibility Inquiry Transaction (Eligibility Inquiry / 270);
- HIPAA Eligibility Response Transaction (Eligibility Response / 271); and
- Explanation of Benefits (EOB).

The Privacy Rule refers to this information as PHI. The scope of PHI includes all patient demographic data that discloses any of the following information:

- the individual's past, present, or future physical or mental health or condition;

- the provision of health care to the individual; or
- the past, present, or future payment for the provision of health care to the individual that identifies the individual or reasonably can be believed to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number). PHI included in the patient medical history is referred to as an Electronic Health Record (EHR). Therefore, an EHR is also protected by the Privacy Rule. The entire Privacy Rule is located at the OCR website (DHHS: Office for Civil Rights, 2013).

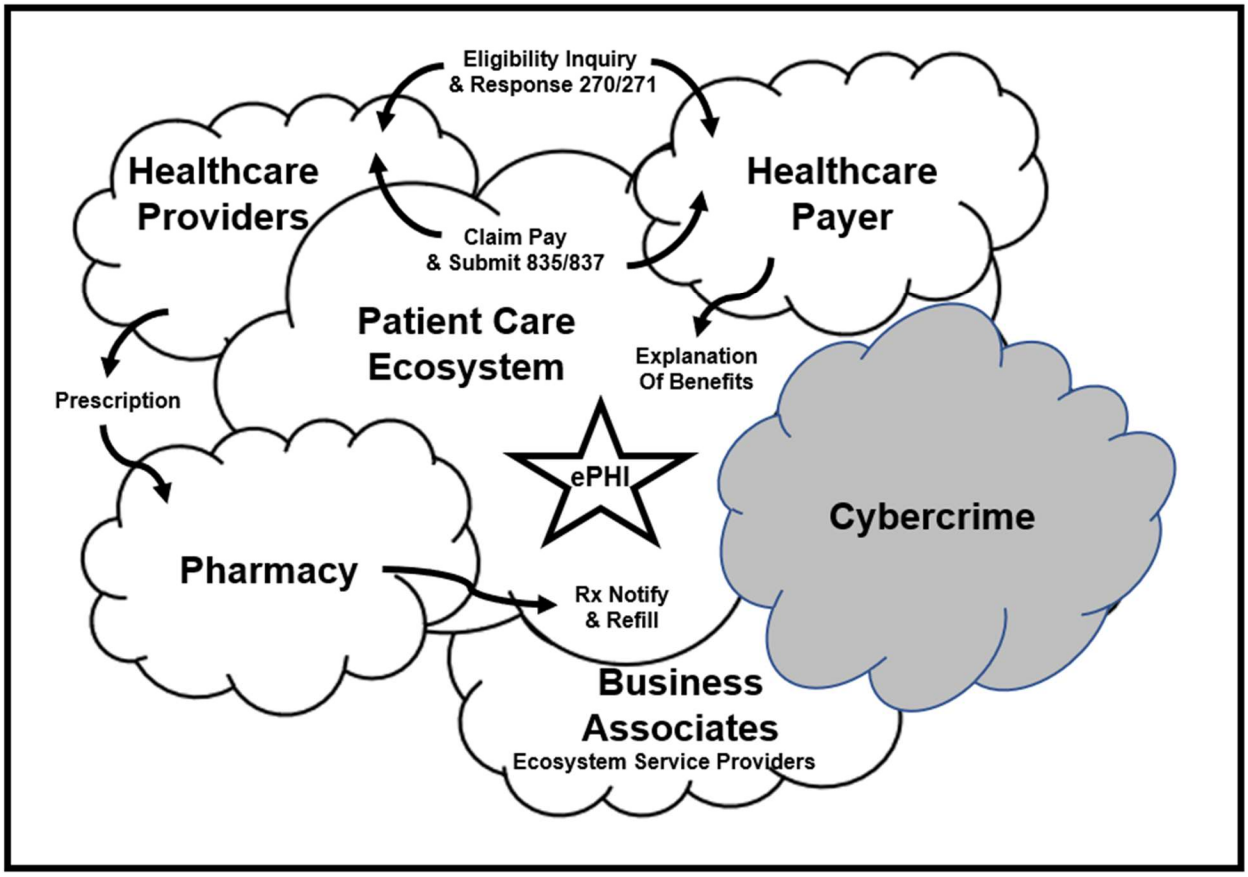

Figure 7. Patient care ecosystem with HIPAA EDI transactions.

While HIPAA and the HIPAA Privacy Rule provide a solid foundation for understanding the healthcare stakeholders impacted and the patient data that qualifies as PHI (the "what" and

the "why"), it does not address protective measures (the "how") that are specifically related to the electronic transmission of digital patient health information. To connect the "what" and "why" with the "how," The Health Information Technology for Economic and Clinical Health (HITECH) Act was signed into law in 2009. "Subtitle D of the HITECH Act addresses the privacy and security concerns associated with the electronic transmission of health information, in part, through several provisions that strengthen the civil and criminal enforcement of the HIPAA rules" (DHHS: Office for Civil Rights, 2017).

In conjunction with HITECH, the OCR has established a close relationship with the National Institute of Standards and Technology (NIST) to develop a crosswalk that maps NIST Cybersecurity best practices to HIPAA's Privacy and Security Rules. The primary goal of the crosswalk was "ensuring the confidentiality, integrity, and availability of electronic protected health information (ePHI) that covered healthcare entities and their business associates create, receive, maintain, or transmit" (DHHS: Office for Civil Rights, 2017). The NIST Cybersecurity Framework Core includes five integrated functions that create a management continuum to address an organization's cybersecurity risk. The OCR and NIST teams collaborated to map each ePHI protection standard and implementation approach in the HIPAA Security Rule on to a related NIST Cybersecurity Framework Subcategory (DHHS: Office for Civil Rights, 2016).

While the entire crosswalk table and its contents should be considered when planning a company's Enterprise Information Security Program and its alignment to the HIPAA Security Rule, this research study focused only on those crosswalk categories and subcategories that directly impacted the privacy and integrity of patient information as it moves from point to point across the Internet through and between covered healthcare entities and their business associates. The key crosswalk focus areas within the scope of this study are shown in Table 1 and are

represented as primary (critical for this study) and secondary (supporting focus area) "areas of relative importance" as related to the protection of patient information. These in-scope focus areas span all five of the NIST Cybersecurity Framework Core Functions: Identify, Protect, Detect, Respond, and Recover. The crosswalk categories and subcategories critical for this research study were those that are directly related to the protection of ePHI when being accessed or processed, whether at rest or in transit. Those critical categories are the following:

- understanding the roles and responsibilities of all covered entities and business associates that process or host ePHI (ID.AM-6 and ID.BE-1);
- understanding data flows throughout the ePHI transaction lifecycle (ID.AM-3);
- management of information and data access controls (PR.AC [1,3,4]);
- implementing an appropriate level of data security (PR.DS [1-7]); and
- the establishment and use of a comprehensive risk assessment framework (ID.RA [1-6]).

Subsequent sections of this literature review explore these focus areas in more detail with the goal of continuing to refine the crosswalk towards the minimum necessary categories needed for the selection criteria and risk factors used to select and leverage a risk assessment model.

Table 1. OCR/NIST crosswalk table (excerpt related to ePHI, only).

Function	Category	Subcategory	Relevant Controls	Relative Importance
IDENTIFY (ID)	Asset Management (ID.AM)	InfoSec roles & responsibilities	COBIT 5, NIST SP 800-53	Secondary
	Business Environment (ID.BE)	Company's role in supply chain	COBIT 5, NIST SP 800-53	Primary
	Governance (ID.GV)	InfoSec policy established	HIPAA Security Rule (HSR)	Secondary
	Governance (ID.GV)	Regulatory requirements	HSR	Secondary
	Risk Assessment (ID.RA)	All Subcategories	COBIT 5, NIST SP 800-53, HSR	Primary
PROTECT (PR)	Access Control (PR.AC)	Identity mgt. established	COBIT 5, NIST SP 800-53, HSR	Primary
		Remote access managed	COBIT 5, NIST SP 800-53, HSR	Primary
		Access – Least privilege	NIST SP 800-53, HSR	Primary
	Awareness & Training (PR.AT)	Privileged users' roles/responsibility	COBIT 5, NIST SP 800-53, HSR	Primary
		Third-party roles/ responsibility	COBIT 5, NIST SP 800-53, HSR	Primary
	Data Security (PR.DS)	Data-at-rest is protected	CCS CSC 17, COBIT 5, NIST SP 800-53, HSR	Primary
		Data-in-transit is protected	CCS CSC 17, COBIT 5, NIST SP 800-53, HSR	Primary
		Assets managed throughout disposition	COBIT 5, NIST SP 800-53, HSR	Secondary
		Protection against data leaks	CCS CSC 17, COBIT 5, NIST SP 800-53, HSR	Primary
		Information Integrity Checking	NIST SP 800-53, HSR	Primary
		Separate production from other environs.	COBIT 5, NIST SP 800-53, HSR	Secondary
		Data destroyed per policy	COBIT 5, NIST SP 800-53, HSR	Secondary
		Protection continuously improved	COBIT 5, NIST SP 800-53, HSR	Primary
	Maintenance (PR.MA)	Remote maintenance is managed	COBIT 5, NIST SP 800-53, HSR	Primary
	Protective Technology (PR.PT)	Protect removable media	COBIT 5, NIST SP 800-53, HSR	Secondary
		Access is least functionality	COBIT 5, NIST SP 800-53, HSR	Primary
DETECT (DE)	Anomalies & Events (DE.AE)	Data flows managed	COBIT 5, NIST SP 800-53, HSR	Primary
	Detection Processes (DE.DP)	Communicate event detection	COBIT 5, NIST SP 800-53, HSR	Secondary
RESPOND (RS)	Communications (RS.CO)	All Subcategories	COBIT 5, NIST SP 800-53, HSR	Secondary
RECOVER (RC)	Recovery Planning (RC.RP)	Recovery plan execution	CCS CSC 17, COBIT 5, NIST SP 800-53, HSR	Secondary

Digital Healthcare Information in the Cloud

As previously mentioned, covered healthcare entities and their business associates are continually challenged to extend their use of cloud computing to improve system integration between them and to help facilitate standardized and safe patient data exchange throughout that patient's medical lifecycle. With an emphasis on the concept of safety, the next section focuses on key points of probable vulnerability for patient data as it moves through the cloud and from stakeholder to stakeholder. First, it is important to develop a common vocabulary for the various cloud deployment models and to show how healthcare stakeholders interact with these models,

as they share patient information that facilitates patient care. A key assumption behind this section of the study is that healthcare stakeholder risk aversion increases as the cloud deployment model selected becomes less controllable by the stakeholder.

To assist with the comprehension of cloud capabilities and components and to ensure that this study was founded on industry standard terminology that can be leveraged for healthcare, this research once again relied on credible guidance from NIST. Specifically, this study considered NIST Special Publication 800-145. NIST created that document to meet regulatory requirements under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347. SP800-145 was created to provide broad comparisons among cloud services and deployment approaches and to establish a baseline for discussion on topics ranging from what cloud computing is to explanations of various cloud computing deployment options (Mell & Grance, 2011). Understanding the various characteristics of cloud computing and service and deployment models is critical for SMBE&A organizations that are seeking to understand and assess the risks associated with cloud computing. By researching cloud-computing models, this study also considered the criteria used to select and leverage a risk assessment model.

Essential cloud characteristics. Cloud computing provides a model for enabling on-demand network access to a shared pool of configurable computing resources that can be quickly deployed and released with minimal effort and often through self-service capabilities. As further defined by NIST, cloud computing is composed of five essential characteristics, three service models, and four deployment models (Mell & Grance, 2011). An abbreviated version of these characteristics and models is depicted at Figure 8. For a computing environment to be considered cloud computing, its environment must include capabilities that are aligned with each of the five essential characteristics discussed below.

1. On-demand self-service - A consumer can automatically and unilaterally provision computing capabilities, such as server time and network storage, as needed without requiring human interaction with each service provider.
2. Broad network access - Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).
3. Resource pooling - The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. Examples of these computing resources include storage, processing, memory, and network bandwidth.
4. Rapid elasticity - Capabilities can be elastically provisioned and released, in some cases automatically, to rapidly scale outward and inward, commensurate to demand.
5. Measured service - Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts).

From this list of five essential characteristics for cloud computing, SMBE&A are most concerned with characteristics that create a perception of loss of control. Those characteristics include resource pooling or multi-tenant and rapid elasticity. While these characteristics are required to support system scaling, growth, and cost control, they also include risks. Therefore, they are often considered candidate factors for the risk assessment model selection findings presented in Chapter 4.

Cloud service models. Cloud service models are essentially containers that include a predetermined set of IT components that the consumer can "rent" from the cloud provider. The reasons for choosing one model over another vary, but they can include budgetary constraints, build versus buy policies, or resource constraints. Standard cloud service models follow.

- Software as a Service (SaaS) - The capability is provided to the consumer to use the provider's applications as they are running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface.
- Platform as a Service (PaaS) - The capability is provided to the consumer to deploy onto a cloud infrastructure for consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.
- Infrastructure as a Service (IaaS) - The capability is provided to the consumer to provision processing, storage, networks, and other fundamental computing resources where the consumer can deploy and run arbitrary software, which may include operating systems and applications.

SMBE&A are less concerned with cloud service models. The perception of service models is that they may provide cost savings. While this perception may be true in theory, when selecting cloud service models, investors must evaluate how service providers are deploying their service offerings. Therefore, these service models were not considered candidate risk factors for the risk assessment model that will be presented in Chapter 4.

Cloud deployment models. Cloud deployment models are options that encapsulate all cloud investments. The reasons for choosing one model over another often have to do with business decisions, such as the level of required privacy, elasticity for unplanned demand,

synergistic opportunities across a consumer population, or the need to have a combination of two or more of those requirements. Listed below are NIST's definitions for each model:

> *Private cloud* - A cloud infrastructure provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units).
>
> *Community cloud* - A cloud infrastructure provisioned for exclusive use by a specific community of consumers for organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations).
>
> *Public cloud* - A cloud infrastructure provisioned for open use by the public.
>
> *Hybrid cloud* - A cloud infrastructure composed of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities but that are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

Among this list of four cloud deployment models, SMBE&A are most concerned with deployment models that create a perception of loss of control. The primary concern about cloud deployment models is user perceptions of the public cloud. While this deployment model is required to support quick deployment, growth, and cost controls, it also includes inherent risk. Therefore, the public cloud deployment model is considered a candidate risk factor in the risk assessment model presented in Chapter 4.

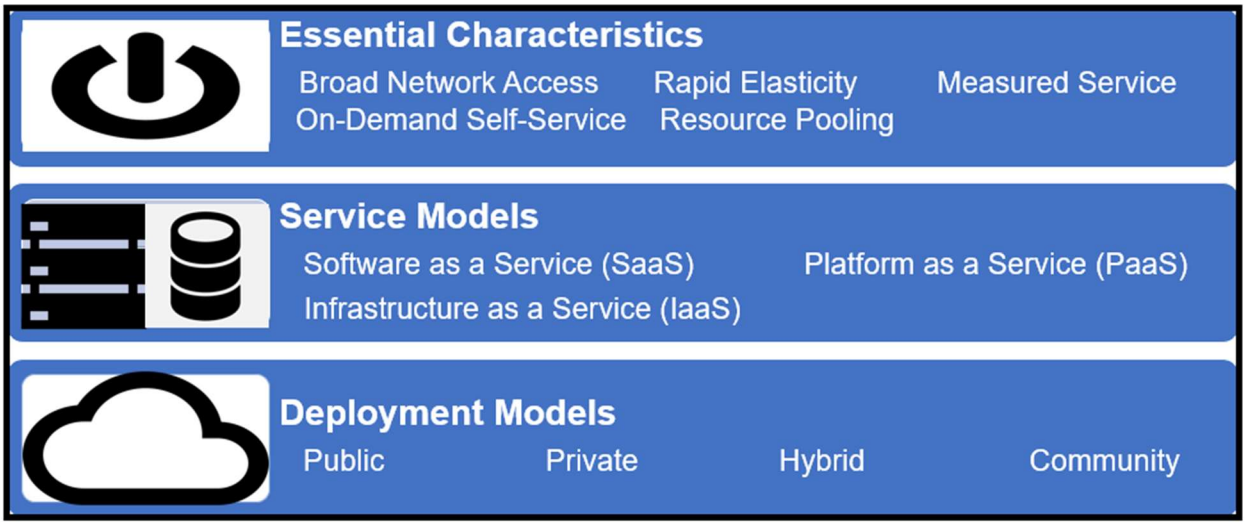

Figure 8. NIST capability model for cloud computing.

Heretofore, a common vocabulary has been developed for the healthcare patient lifecycle, HIPAA requirements, and cloud computing models that support covered entities and business associates. The following section considers the research in aggregate with the goal of revealing technical risk factors associated with data breaches as related to ePHI being compromised by cybercriminals. For example, technical risk factors related to ePHI include the "at rest" and "in transit" states as data are being processed by the SMBE&A population in the cloud. To acknowledge possible points of vulnerability for ePHI in the cloud, it is important to consider the standard patient treatment and payment transactions depicted in Figure 7, which includes patient information as it travels between a healthcare patient and a SMBE&A population sample.

As previously assumed, healthcare stakeholder risk aversion increases as the cloud capability characteristics and deployment model selected become less controllable by the stakeholder. Less stakeholder control is typically associated with the essential cloud characteristics of rapid elasticity and resource pooling/multi-tenancy, as these characteristics can be associated with the haphazard expansion or reduction of cloud assets or inadequately protected multi-tenant cloud resource consumption. The biggest cloud deployment concern from

healthcare stakeholders emerges when a public cloud deployment model is used. It is generally believed that the greatest loss of stakeholder control occurs when public cloud assets are used to process confidential information, as a public cloud is often used for rapid and unplanned growth scenarios that may be less restrictive and, therefore, less protected (Farahmond, 2010, pp. 1-7).

Layered Protective Architecture: Defense in Depth Approach

To select and leverage a risk assessment model that can assist the SMBE&A population with assessing the risks associated with ePHI in either the at-rest or in-transit states, this study considered additional technical risk factors. Taking guidance from the HIPAA/NIST crosswalk (Table 1) and coupled with the complexities of processing ePHI in disparate cloud deployment scenarios (Figure 8), a layered technical architecture should be leveraged to assist SMBE&A with the further development of candidate technical risk factors to be used with a selected risk assessment model. In this section of the study, research was conducted on a layered architecture framework that assists with the identification of candidate technical risk factors.

In the U.S., the National Security Agency (NSA) has developed a framework that supports a layered protective architecture called Defense in Depth (DiD). The Information Assurance Department (IAD) of the NSA (2015) developed DiD to be a pragmatic framework that assists IT security professionals with information assurance initiatives. The scope of the DiD Strategy is balanced across three primary domains (Figure 9), which are People, Technology, and Operations, defined as follows:

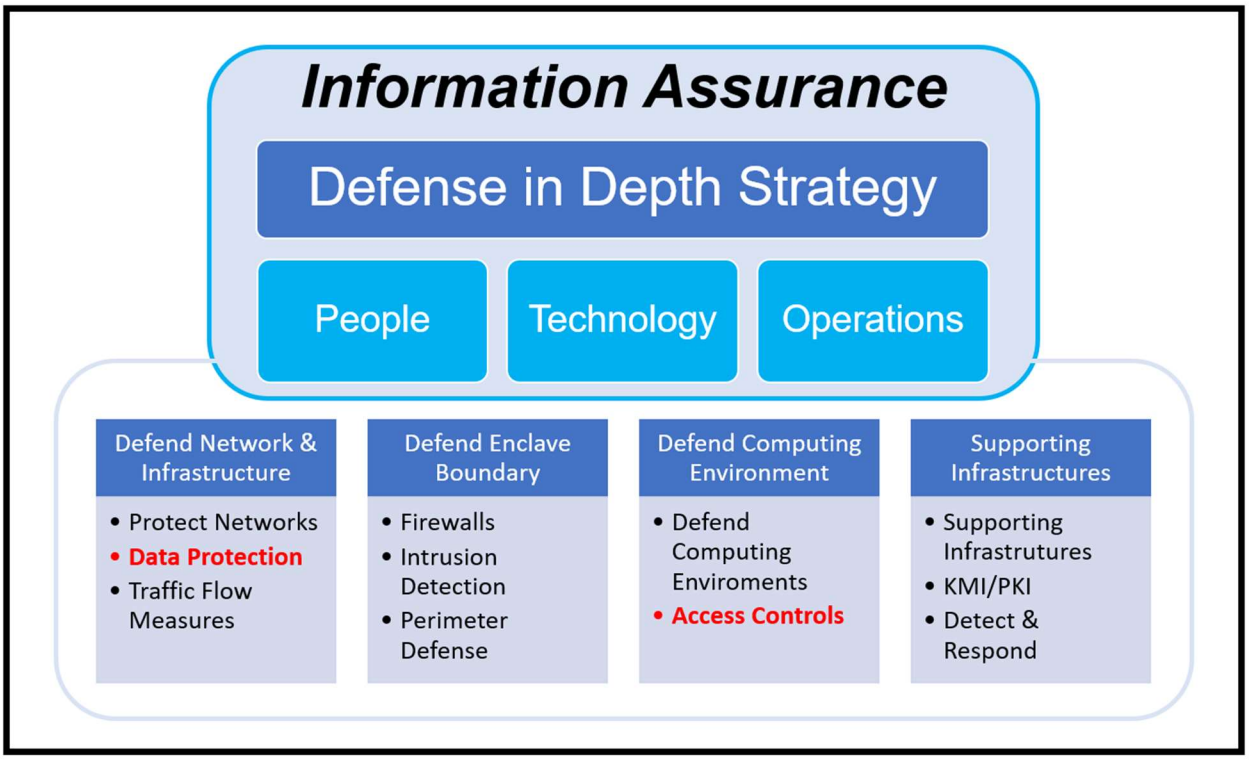

Figure 9. NSA DiD strategy with four key focus areas.

- People – Effective Information Assurance policies and procedures supported by senior executive leadership and followed by the entire organization.
- Technology – Information Assurance policies, procedures, and architectural direction that help to ensure that the most appropriate technology solutions are procured and deployed.
- Operations – Daily activities required to make sure an organization's security posture is sustainable.

Because cybercriminals exploit targets from multiple points, organizations must deploy defensive postures across multiple locations. As depicted in Figure 9, four foundational focus areas should be included in planning for enterprise defensive postures. Given that the scope of this research is the protection of ePHI as it is being hosted and processed, the DiD focus areas

that address data encryption and access controls that have been researched here are highlighted in red font (Figure 9).

Data protection. With guidance from the OCR/NIST Crosswalk Table (Table 1) and the NSA DiD Framework (Figure 9), this study considered research on various data encryption requirements and controls that assist with providing data protection measures that include confidentiality and integrity for ePHI and Electronic Medical Record (EMR) data this is transmitted over distributed networks. These requirements and controls for data encryption were used to help identify encryption methods in DiD that translate well into candidate technical risk factors for use with a selected risk assessment model. To understand specific encryption guidance, this study first investigated the Data Security (PR.DS) category of the Protect function in the OCR/NIST Crosswalk (Table 1). In this crosswalk category, "Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information" (DHHS: Office for Civil Rights, 2016).

Within the PR.DS category, there are subcategories that relate to detailed controls for data at rest (PR.DS-1) and data in transit (PR.DS-2). SC-28 defines data at rest as the state of information when it is located on storage devices as specific components of information systems (NIST, 2014). SC-28 offers cryptography to protect ePHI and states that organizations may employ different mechanisms to achieve confidentiality and integrity protections, including the use of cryptographic mechanisms. SC-8 defines a data in transit control as applying to both internal and external networks and all types of information system components from which information can be transmitted. This control is particularly challenging to implement because ePHI and EHR data are often in transit across numerous distributed cloud-based systems as they move through a patient's healthcare lifecycle (depicted in Figure 7).

Taking direction from the HIPAA Privacy Rule and protective guidance from DHHS, NIST, and NSA to frame a search, this study explored available research on encryption options for at-rest and in-transit ePHI. Cloud service providers Online Tech (2013) describes at-rest and in-transit ePHI, respectively, as follows:

- ePHI data at rest is all electronic personal health information that is not in movement on a system, end user device, or storage media;
- ePHI data in transit is all electronic personal health information that is in movement, traveling across integration points either across the Internet or within a private network; and
- encryption for data at rest or in transit can be applied to one or many files.

Listed below are several encryption deployment options and techniques for both at-rest and in-transit ePHI (Online Tech, LLC, 2013):

Within the subject of ePHI at rest, the concept of authentication refers to encrypted stored data that requires users to verify their identity and authenticate to gain access (covered in the access controls section). Another key concept of ePHI at-rest is data backups. While storing backups at an offsite location is good practice for organizations in case of a disaster, data at rest must also be encrypted and secured. Following are some common encryption options for ePHI at rest.

- *Full disk encryption (FDE)* is the encryption of all data on a hard drive used to boot a computer.
- *Database-level encryption* is the process of encrypting data as it is written to and read from a database.

- *Application-level encryption* allows for more granular and custom encryption of data, meaning that the application can identify what sensitive data to encrypt and has insight into which users have what kind of access.

Following are common deployment options for ePHI in transit.

- *Virtual Private Network (VPN)* – Data are encrypted when sent from one network to another; a VPN server then decrypts the data and forwards it to the receiving server.
- *Secure Sockets Layer (SSL)* – SSL is a cryptographic protocol that can provide security as information is transmitted over the Internet. It should be noted that SSL has been replaced with Transport Layer Security (TLS).
- *Secure File Transfer Protocol (SFTP)* – SFTP allows for secure file transfers between hosts as well as for the access/management of files on remote file systems

Because all encryption methods listed meet the control guidelines from HIPAA/NIST crosswalk subcategories PR.DS-1 (data at rest) and PR.DS-2 (data in transit), all methods are candidate technical risk factors that may be used for the risk assessment model selection presented in Chapter 4.

It should be emphasized here that this study focused on controls related to ePHI at rest and in transit, namely encryption methods. However, specific encryption implementation details are out of scope for this study.

Access controls. With guidance from the OCR/NIST Crosswalk (Table 1) and the NSA DiD Framework (Figure 9), this study considered research on various data access control approaches that assist with providing confidentiality and integrity for ePHI and EMRs transmitted over distributed networks. These requirements for access controls were used to help identify access control methods in DiD that translate well into candidate technical risk factors

and may be considered for use with a selected risk assessment model. To understand specific guidance around access controls, this study first investigated the Access Control (PR.AC) category of the Protect function in the OCR/NIST Crosswalk (Table 1).

Within category PR.AC, there are subcategories that address detailed controls for Identity Management (PR.AC-1), Remote Access (PR.AC-3), and Least Privilege and Separation of Duties (PR.AC-4). This crosswalk category indicates that "access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions" (DHHS: Office for Civil Rights, 2016).

- *Identity Management.* (PR.AC-1) - Identities and credentials are managed for authorized devices and users. Two examples of Identity Management include Multi-Factor Authentication and Authorization. Role-based Access (RBAC) can be leveraged to accomplish authorization.
- *Remote Access.* (PR.AC-3) - Remote access is managed as defined in PR.AC-4. (Souppaya & Scarfone, 2016, p. 3). Examples of Remote Access include Virtual Private Network (VPN), Remote System Control, and Individual Application Access.
- *Least Privilege and Separation of Duties (LPSD)*. (PR.AC-4) - Access permissions are managed by incorporating the principles of least privilege and separation of duties. An example of LPSD is Authorization Provisioning, which can be achieved by using a RBAC system approach.

As recommended by NSA in the DiD framework, it is necessary to defend the computing environment that hosts or processes ePHI with multi-factored authentication and role-based access controls on hosts, servers, and applications to resist insider, close-in, and distribution attacks. Multi-factor authentication is critical to mitigating the risks associated with automated

cybercrime. Using a password-only (single-factor) approach to authentication is not sufficient, as there are numerous password hacking approaches that can easily discover and exploit passwords. At minimum, information security professionals should also include some type of biometric or randomly generated digital key to accompany passwords to achieve multi-factor authentication. RBAC enables LPSD capabilities by greatly reducing the possibility of an undesirable combination of access permissions that could weaken the security posture for a system or application (O'Connor & Loomis, 2010).

Because all access control methods listed meet control guidelines from the HIPAA/NIST crosswalk subcategories PR.AC-1 (identity management), PR.AC-3 (remote access), and PR.AC-4 (least privileged access), all methods are potential candidate technical risk factors that may be used for the risk assessment model selection findings presented in Chapter 4. It should be emphasized here that this study focused on controls related to access to ePHI: namely, access control methods. However, specific access control implementation details are outside the scope of this study.

Risk Assessment Requirements and Methods

Thus far, the literature review for this study has focused on HIPAA requirements for the protection of ePHI and a variety of variables that introduce, identify, or mitigate risk related to ePHI that is processed in the cloud by the SMBE&A population. This section of the literature review shifts to considerations of risk analysis and management best practices and discusses the research conducted for risk assessment models and methods. David Wagner, CEO of Country Risk Solutions (2018), offered the following comments on assessing and managing risk:

> Some risks that we believe are unknown, are not unknown. With some insight and forward planning, risks that are usually difficult to foresee can be seen or predicted.

> When equipped with the right capabilities, knowledge, and insight, risk variables and factors are more visible, which allows us to better assess and manage them. (p. 5)

Wagner's thoughts on risk translate well to risk assessment related to ePHI and the processes, tools, and variables leveraged for that kind of assessment. This section used the previous literature research in this study to (a) consider risk analysis best practices that align with the HIPAA Security Rule and guidance from NIST and (b) research risk assessment models and methods that align with HIPAA requirements and guidance from NIST and there were, therefore, probable candidates for evaluation by the selection process introduced in Chapter 3.

HIPAA security rule requirements. The HIPAA Security Rule requires healthcare covered entities and business associates to assess risk and implement appropriate protective measures to protect ePHI from becoming compromised (DHHS: Centers for Medicare & Medicaid Services, 2007). To further support the Security Rule by providing more specific guidance, the Centers for Medicaid and Medicare Services (CMS) created the HIPAA Security Series Papers. "This publication of papers includes a series of seven studies which all focus on specific aspects of the Security Rule" (DHHS: Centers for Medicare & Medicaid Services, 2007). The CMS study focused on the series paper titled "Basics of Risk Analysis and Risk Management," using them as a guide for choosing appropriate risk assessment models and tools. The CMS Risk Analysis and Risk Management section of the HIPAA Security Series (2007) states that a covered entity must conduct deliberate risk assessments and practice thorough risk management to identify and mitigate possible vulnerabilities associated with ePHI.

While the HIPAA Security Rule does not prescribe specific risk analysis or risk management methodologies, the Basics of Risk Analysis and Risk Management paper within the HIPAA Security Series does derive much of its guidance from NIST SP 800-30, Risk

Management Guide for Information Technology Systems. CMS offers steps from NIST SP 800-30 to provide guidance to covered entities and business associates that are planning for and choosing their risk analysis or risk management methodologies. Those steps form the basis for conducting requirements analysis of risk analysis and management. The following steps highlight the key elements of risk analysis:

1. Identify the scope of the analysis;
2. gather data;
3. identify and document potential threats and vulnerabilities;
4. assess current security measures;
5. determine the likelihood of threat occurrence;
6. determine the potential impact of threat occurrence;
7. determine the level of risk; and
8. identify security measures and finalize documentation (DHHS: Centers for Medicare & Medicaid Services, 2007).

The risk analysis steps provided by CMS and NIST were used in this study to help develop the selection criterion for risk assessment models and capabilities. Those selection criteria were clearly defined and leveraged in a risk management model selection process in the methodology chapter (Chapter 3) of this study. Because the estimation of risk is not an exact science, the methodologies used to evaluate risk often mix of qualitative and quantitative approaches. Considering the guidance from OCR (HIPAA Security Rule), CMS, and NIST, this study focused research on widely used risk assessment methodologies and tools that rely upon a blend of numerical and categorical variables and outcomes to arrive at conclusions about risk levels. Because this research is focused on risk assessment models, broader development of a

comprehensive risk management plan and maintaining security measures are outside the scope of this research.

Risk assessment methodologies and capabilities. There are many options for assessing, analyzing, and managing the risks associated with IT assets. Richard E. Mackey, Jr. vice president of consulting at SystemExperts, an information security-services firm, in his article titled "Choosing the Right Information Security Risk Assessment Framework," argued, "The heart of a risk assessment framework is an objective, repeatable methodology that gathers input regarding business risks, threats, vulnerabilities, and controls and produces a risk magnitude that can be discussed, reasoned about, and treated" (Mackey, 2011). However, risk management can easily become an overwhelming undertaking that involves a large investment of resources, people, technology, and money.

Risk management approaches can include everything from high-level qualitative assessment to laborious and time consuming quantitative efforts. A right-sized hybrid approach is often a reasonable way forward. As Whitman and Mattord (2017) explained, the goal of a hybrid assessment is to expand on qualitative-only measures without resorting to unconfirmed estimations. After further refinement of the scope for risk management capabilities to those required for SMBE&A to satisfy the HIPAA Security Rule and to fit within the guidance provided by CMS via NIST SP 800-30 R1, this study considered a smaller list of risk assessment model options that is easier to comprehend.

To establish a starting point for the discovery of models and methods, the study researched and leveraged the Inventory of Risk Management and Risk Assessment Methods provided by the European Union Agency for Network and Information Security (European Union Agency for Network and Information Security [ENISA], 2018). ENISA is a center of

expertise for cybersecurity in Europe. Given the complexity of addressing cybersecurity across the diverse states of the European Union, this source is appropriate for considering risk management methods used worldwide and supports the research goals of this study. The risk assessment methods considered in this research and published by ENISA are as follows:

- Octave-S v1.0 for SMB's: The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE®) risk assessment model was developed by the Software Engineering Institute of the Carnegie Mellon University. The U.S. Department of Defense first invested in this initiative to address HIPAA security standard compliance requirements. OCTAVE can be customized to the meet the technical and business needs of each organization (Gritzalis, Iseppi, Mylonas, & Stavrou, 2018).

  OCTAVE is a self-directed approach, which means that people from an organization assume responsibility for setting the organization's security strategy. The traditional OCTAVE method includes three phases, shown in Figure 10. In phase 1, the analysis team identifies important information-related assets and the current protection strategy for those assets. The team then determines which of the identified assets are most critical to the organization's success, documents their security requirements, and identifies threats that can interfere with meeting those requirements. In phase 2, the analysis team performs an evaluation of the information infrastructure to supplement the threat analysis performed in phase 1 and to inform the mitigation decisions in phase 3. Finally, in phase 3, the analysis team performs risk identification activities and develops a risk mitigation plan for the critical assets.

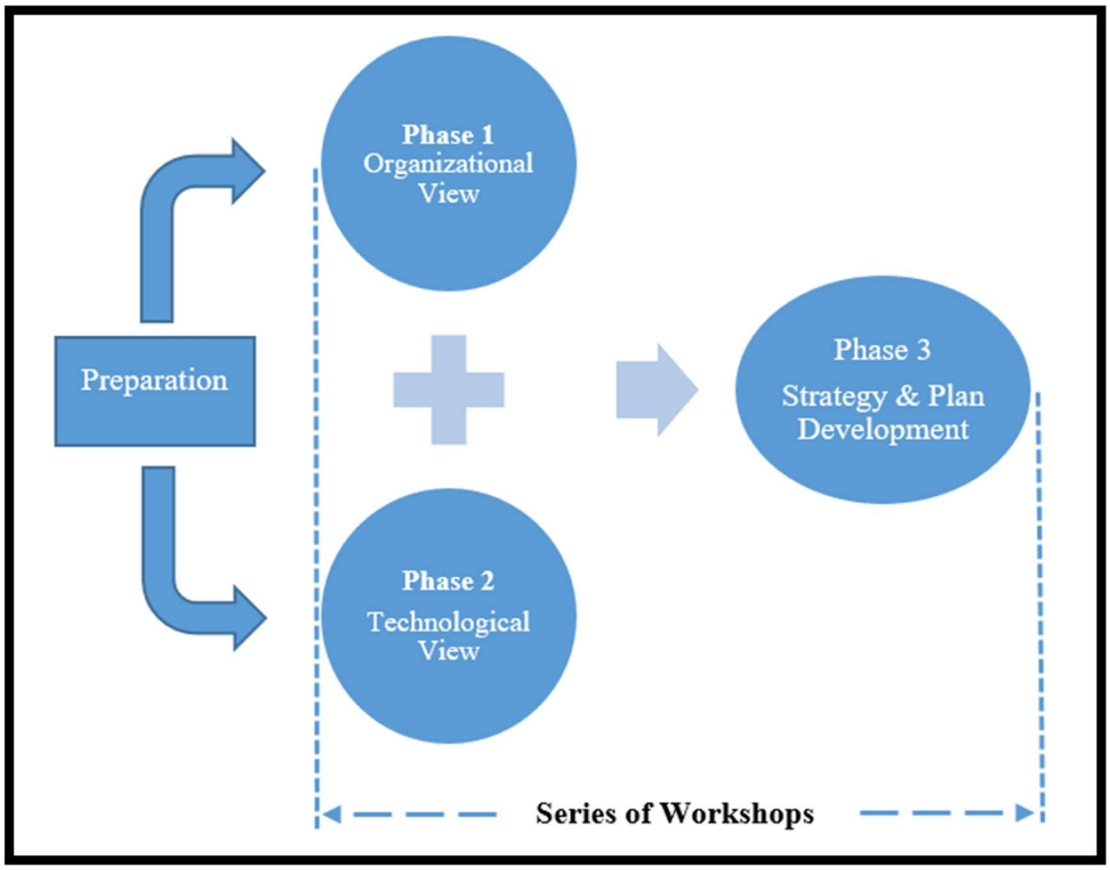

Figure 10. Octave method phases.

The traditional OCTAVE method was established for medium to larger sized companies and, while it is a widely used methodology, it is labor and process intensive and can overwhelm a smaller company.

OCTAVE-S is an alternative form of the original OCTAVE model that is tailored to smaller organizations (those with fewer than 100 people) that have limited resources. OCTAVE-S is typically led by a small, cross-functional team (of three to five employees) that collects and analyzes information to develop a strategy and execution plan that addresses the specific needs of the company being evaluated (European Union Agency for Network and Information Security [ENISA], 2018). Another significant feature of OCTAVE-S is that it is more structured than the OCTAVE method. Security concepts

are embedded in the OCTAVE-S worksheets and guidance, allowing less experienced risk and security practitioners to address a broad range of risks with which they may be familiar. A final distinguishing feature of OCTAVE-S is that it requires a less extensive examination of an organization's IT infrastructure (Caralli, Stevens, Young, & Wilson, 2007).

- *ISO/IEC IS 13335-2:* An ISO standard describing the complete process of information security risk management in a generic manner. The annexes contain examples of information security risk assessment approaches as well as lists of possible threats, vulnerabilities, and security controls. ISO/IEC IS 13335-2 can be viewed as the basic information risk management standard at an international level, one that sets a framework for defining the risk management process. NIST SP 800-30, Revision 1, as previously discussed, gives very detailed guidance on identifying what should be considered within the realm of computer security risk management and risk assessment. It provides some detailed checklists, graphics (including flowchart), and mathematical formulas, as well as references that are mainly based on U.S. regulatory issues.
- *Open Web Application Security Project (OWASP):* An open community dedicated to enabling organizations to conceive of, develop, acquire, operate, and maintain applications that can be trusted (Open Web Application Security Project [OWASP], 2018). All OWASP tools, documents, forums, and chapters are free and open, making them an excellent choice for SMBs with limited resources. OWASP is governed worldwide by their foundational bylaws, core values, and code of ethics, which can all be reviewed at the OWASP website.

The standard risk model used by OWASP states that [Risk = Likelihood * Impact]. With that formula in mind, six steps that comprise the OWASP approach. In these steps, the factors that make up "likelihood" and "impact" are broken down. An introduction to and brief definitions of the six steps are provided below (Open Web Application Security Project, 2016).

1. Identifying a Risk*:* Identify a risk that needs to be rated. The attributes of the risk being identified should include the threat agent involved, the attack that will be used, the vulnerability involved, and the impact of a successful exploit on the business.
2. Factors for Estimating Likelihood*:* This is a rough measure of how likely this vulnerability is to be uncovered and exploited by an attacker. It is not necessary to be over-precise in this estimate. Generally, identifying whether the likelihood is low, medium, or high is sufficient.
3. Factors for Estimating Impact: The OWASP approach considers two impact categories. The first is the "technical impact" on the application, the data it uses, and the functions it provides. The other is the "business impact" on the business and the company operating the application.
4. Determining Severity of the Risk: In this step, the likelihood estimate, and the impact estimate are summed to calculate an overall severity for the severity of the risk.
5. Deciding What to Fix: After the risks to the application have been classified, there will be a prioritized list of what to fix. As a rule, the most severe risks should be fixed first. It simply does not help the overall risk profile to fix less important risks, even if they are easy or cheap to address.

6. Customizing a Risk Rating Model: Having a customizable risk ranking framework for a business is critical. A tailored model is much more likely to produce results that match perceptions of a serious risk. This is particularly critical for assessing the risk of ePHI where the expectations are clearly spelled out in the HIPAA privacy rule and stakeholder perceptions are known.

Figure 11 illustrates a completed risk rating exercise using the OWASP methodology for a typical Network Penetration Test result use case.

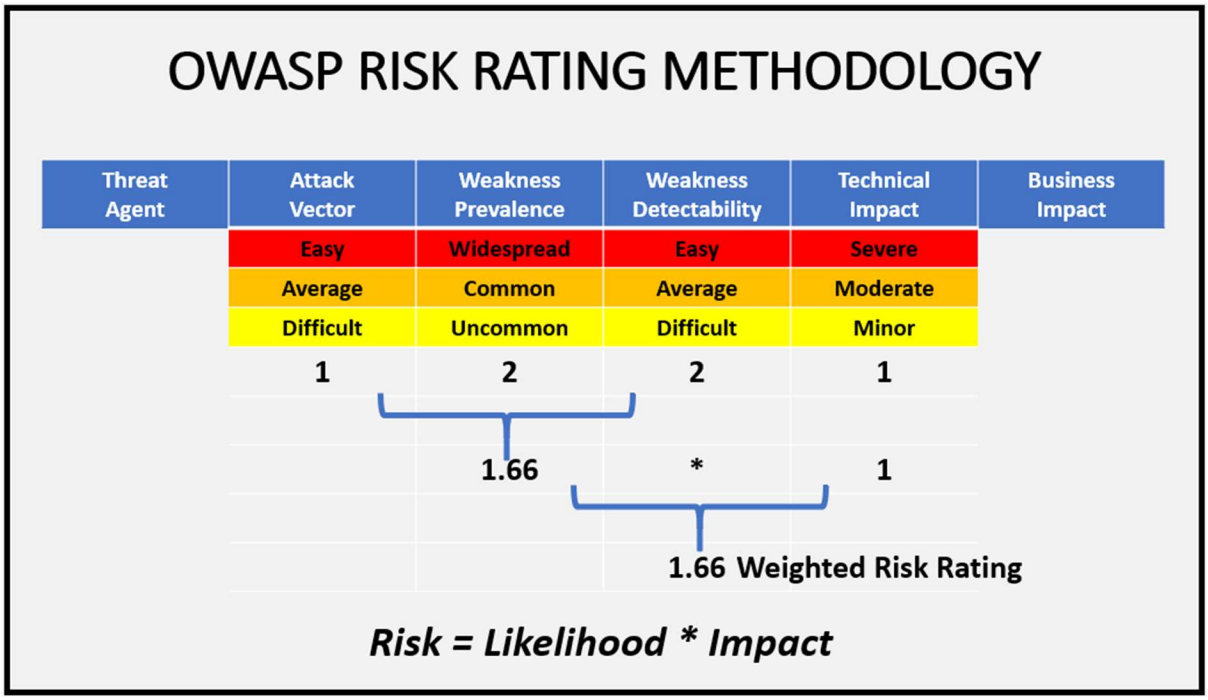

Figure 11. OWASP risk ratings for PEN test use case example.

A supplemental tool that can be used in a supporting role with most risk assessment methods is the Security Risk Assessment (SRA) Tool offered by the Office of the National Coordinator for Health Information Technology (ONC, in collaboration with OCR and OGC), which is available at the HealthIT.gov website. "The purpose of a risk assessment is to identify conditions where Electronic Protected Health Information (ePHI) could be disclosed without proper authorization, improperly modified, or made unavailable when needed" (DHHS: ONC, 2014). Responses to

the questions in the SRA Tool can be used to help with the risk identification, determining the severity and customization steps to be taken for the chosen risk assessment methodology. Specific uses or experimentation for the SRA Tool is beyond the scope of this study, however.

Solution Selection Approach

Decision matrix model. When SMBE&A are considering a best-fit risk assessment model for their organization, they should use a solution selection method that supports fact-based decision making. For this study, a decision matrix approach was used.

Background. The American Society for Quality (ASQ) defines a Decision Matrix Model (DMM) as a framework that "allows teams to evaluate and prioritize a list of options. The team first establishes a list of weighted criteria and then evaluates each option against those criteria" (Tague, 2004). There are several approaches that can be used to develop and leverage a decision matrix. All those approaches use selection criteria to work towards an optimal solution. The differences in approaches lie in the way that each criterion is evaluated for selection. The simplest way to provide value to each criterion is to use broad, highly subjective ranking, as in 1, 2, 3 (1 = low, 2 = medium, 3 = high). More deliberate and less subjective approaches include applying weighted values to each criterion to ensure that the most critical criteria are not overlooked, or something like the Pugh matrix can be used to evaluate new options against an establish a baseline, which may be one of the alternatives or the current product or service. With this approach, the team compares new options against a known baseline.

DMM selection and why. For this study, a weighted criterion approach was selected to assist with the evaluation and selection of a risk assessment methodology. Given an assumption that most SMBE&A are new to the risk assessment process, this population is not likely to have

an established baseline. Otherwise, the Pugh matrix (Tague, 2004) approach would have been further considered.

DMM populated with chosen selection criterion. Table 2 shows the decision matrix that was used in this study. It includes the weighted criteria and placeholders listed as options 1-3 that were then replaced with evaluated risk assessment methodology options in Chapter 4. Also, in Chapter 4, all risk assessment methodologies were evaluated, and the resulting chosen option was presented based on the chosen option being evaluated as the best fit for the SMBE&A population, which processes ePHI in the cloud.

Table 2. Decision matrix template with weighted criteria.

Weighted Criteria Solutions	Flexibility Weight = 4	Low Cost & Complexity Weight = 4	Threat & Vulnerability Weight = 2	Technical Impact Weight = 3	Business Impact Weight = 5	Score Totals
Option-1	Rank = 3 W x R = 12	Rank = 3 W x R = 12	Rank = 1 W x R = 2	Rank = 2 W x R = 6	Rank = 3 W x R = 15	47
Option-2	Rank = 1 W x R = 4	Rank = 1 W x R = 4	Rank = 3 W x R = 6	Rank = 2 W x R = 6	Rank = 2 W x R = 10	30
Option-3	Rank = 2 W x R = 8	Rank = 2 W x R = 8	Rank = 2 W x R = 4	Rank = 2 W x R = 6	Rank = 2 W x R = 10	36

In the DMM example in Table 2, "Business Impact" has been weighted with 5 points, showing that the evaluation team, in this example, considers it the most important criterion compared to others, which are weighted with values less than 5. The team also chose an option rating scale of high = 3, medium = 2, and low = 1. For example, in "Option 1," flexibility is high (3) because that solution option is highly customizable. Option 1 also has a high (3) rating for low cost and complexity, as it is free and requires minimal effort to set up and use. Threat and Vulnerability rated low (1) because those risk factors assume that tooling is in place to populate them in the methodology. Technical Impact has a medium (2) rating, as this risk factor assumes

that some level of security tooling is in place but not mandatory. Business Impact is high (3) because risk factors can be weighted in favor of business factors when it is known that business factors outweigh all other risk factors when assessing risk level.

Each rating is then multiplied by the weight for that criterion. For example, "Flexibility" (with a weight of 4) for Option 1 rates high (3), yielding a score of 12 (4 x 3). After all options have been evaluated and scored, the scores are then added across the rows to obtain a total score for each solution option. Option 1 has the highest score at 47, which is far higher than the next nearest score, which is for Option 3, with a score of 32. Given the relatively large delta between these scores, confidence is increased for Option 1, which has a high likelihood of being a strong fit for the business needs identified in this section of the study.

Other decision matrix considerations.

- "A very long list of options can first be shortened with a tool such as list reduction or multi-voting" (Tague, 2004).
- "Criteria that are often used fall under the general categories of effectiveness, feasibility, capability, cost, time required, support or enthusiasm (of team and of others)."

The following are other commonly used criteria:

For selecting a problem or an improvement opportunity:

- Within control of the team;
- Financial payback;
- Customer pain caused by the problem; and
- Urgency of the problem.

For selecting a solution:

- Root causes addressed by this solution;
- Time until solution is fully implemented;
- Cost to maintain (total cost of ownership); and
- Effect of other systems.

Summary for Literature Review

This literature review highlighted the justification for SMBE&A to leverage a viable risk assessment model to assist with the identification and reduction of risk for ePHI that is processed on the Internet. To accomplish this, many related subject areas were researched, including industry surveys and scholarly research, HIPAA and its regulatory implications for ePHI and SMBE&A, awareness of concerns related to some specific cloud characteristics and deployment models, vulnerabilities associated with ePHI being processed in the cloud, a layered protective architecture discussion required to understand and evaluate technical risk factors related to ePHI vulnerabilities, risk assessment models that help to identify and evaluate ePHI vulnerabilities, and a solution selection using a decision matrix approach.

Computer systems that process ePHI transactions are spread throughout the healthcare ecosystem and are managed with varying degrees of discipline, capability, cost, and risk. These points, coupled with the mass movement of healthcare information being migrated to various cloud hosting and application deployment models, makes ePHI a prime target for cybercriminals. This constraint makes it challenging for U.S. healthcare organizations to achieve an ideal patient care ecosystem, which requires "the consolidation of patient data for broad and comprehensive access (by healthcare providers) that will lead to better patient outcomes, lower costs, and a more efficient healthcare system" (Robichau, 2014). The conundrum is that the value proposition for

an open and efficient healthcare system is in direct conflict with regulatory requirements that protect ePHI and addresses the pervasive cybercrime that makes those requirements necessary.

One possible solution to this problem is to ensure that all SMBE&A are using ePHI protective capabilities that are HIPAA compliant. The presence or absence of such capabilities can be best discovered through strong risk assessment methods and practices. The literature reviewed in this chapter included several risk assessment frameworks that are likely good candidates for the SMBE&A population. In the next chapter (Chapter 3), a research design is leveraged that includes data collection and analysis approaches that help answer research questions related to development of selection criteria and are then used to suggest the best risk assessment methods for SMBE&A with limited resources and that process ePHI on cloud-based systems.

CHAPTER 3. METHODOLOGY

Introduction

In this chapter, the research approach, design, and data analysis used to address the four research questions outlined in Chapter 1 and to analyze associated literature review data from Chapter 2 are described and developed. For example, as shown in the research conducted in Chapters 1 and 2, points of view in the U.S. regarding the protection of ePHI clearly include high anxiety due to the perceived loss of control associated with hosting and processing ePHI in the cloud. Given that pragmatic responses come forward out of actions, situations, and consequences rather than only preceding conditions, a pragmatic research design approach is appropriate for this study (Creswell, 2014). Further, this study is primarily focused on healthcare in the U.S., so the research design is refined from a broad pragmatic point of view to address specific pragmatic problems in the U.S. healthcare industry. The study employed a pragmatic approach that emphasized the research problem and used both qualitative and quantitative methods to understand the problem and answer the research questions presented in Chapter 1. The key characteristics of pragmatism emphasized in this study include considering the consequences of actions, a problem-centered emphasis, and an orientation toward real-world practice. While pragmatism is often associated with mixed methods studies, it is being leveraged in this study to support a hybrid research approach that includes components of convergent mixed methods and case study approaches: It emphasizes processes, activities, and events.

As HIPAA regulations require, SMBE&A must remain aware of risk levels for ePHI to support risk mitigation and HIPAA compliance efforts (DHHS: Office for Civil Rights, 2017). As an industry best practice and with direct guidance from OCR and NIST, impacted SMBE&A can get guidance on conducting IT risk assessments and using the assessment outcomes to

implement appropriate risk mitigations. In this chapter, the methodological approaches applied are used to develop research design and methods that, in turn, are used to justify the need for risk assessment and to select a risk assessment model that is best suited to help SMBE&A to meet HIPAA compliance requirements.

Research Questions

As described throughout this study's background, purpose, and literature review, SBME&As are at risk of HIPAA data (ePHI) breaches. Therefore, they require the ability to select and leverage an appropriate risk assessment model to be able to assess risks to ePHI that is processed within cloud-based systems. To define and support the research required for this study, a research design that includes both qualitative and quantitative data was used. The areas of focus for this design are presented here as the research questions (RQ):

RQ1: Does risk of an ePHI breach justify the need to leverage a viable risk assessment model for the SMBE&A population?

RQ2: Through evaluation and assessment of HIPAA regulatory requirements and impacted IT architecture, what are the current risk factors for risk assessment that are critical for the SMBE&A population?

RQ3: Through evaluation and assessment of current risk models that meet HIPAA risk factor needs, what are candidate models for the SMBE&A population?

RQ4: What selection decision capability can be used by the SMBE&A population to evaluate and select an appropriate risk assessment model and how can the chosen model be leveraged to evaluate risk levels?

The research design for this study used Research Areas (RA1-4) to support resolutions of RQ1-4. The document and data analysis are organized by research areas, as follows:

RA1 for RQ1: The research presented in Chapters 1 and 2 regarding Internet growth and related vulnerabilities justifies the need to leverage an appropriate risk assessment model for SMBE&A.

RA2 for RQ2: Research presented in Chapter 2 regarding HIPAA regulatory requirements and enforcement, along with guidance from NIST and NSA (DiD), identifies related characteristics and risk factors that were later used in this study to evaluate, select, and utilize an appropriate risk assessment model for the SMBE&A population.

RA3 for RQ3: Research presented in Chapter 2 identifies and evaluates risk assessment models that are likely selection candidates for the SMBE&A population.

RA4 for RQ4: Research completed and presented in Chapter 2 identifies and demonstrates an effective decision matrix process that is later used in this study to evaluate and select a risk assessment model that is appropriate for the SMBE&A population.

Research Design

The key components of this research design are illustrated in Figure 12. They include the research approach, research design, data analysis, and approaches to data interpretation.

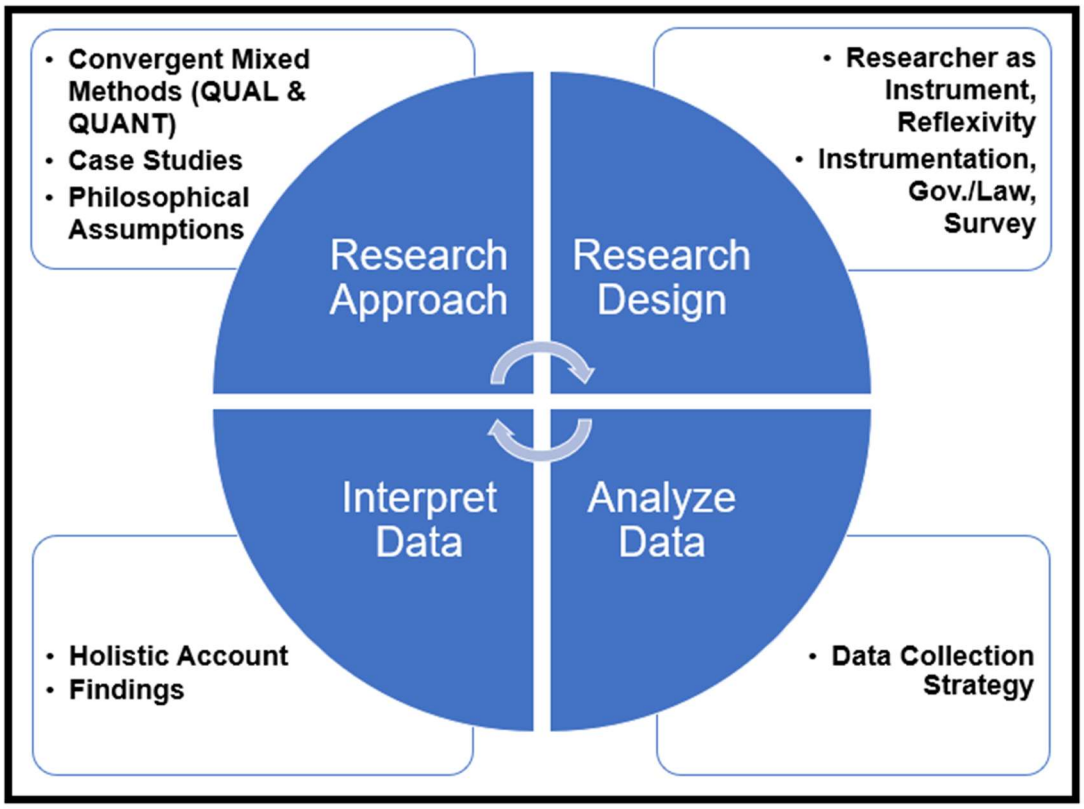

Figure 12. Research design components.

To address the research questions and areas of research, a combination of both qualitative and quantitative information that gathered from the documents researched were leveraged for this study. The following characteristics are associated with each of these information types:

- Qualitative Information
    - researcher as a key instrument,
    - holistic account, and
    - reflexivity.
- Quantitative Information
    - Surveys that include statistical information.
    - Regulatory requirements.
    - Decision-making processes and instrumentation.

- Document Analysis (by theme or grouping)
    - Industry surveys, articles, reports, and scholarly research that confirm risks on the Internet for SMBE&A.
    - HIPAA regulatory requirements and enforcement.
    - DHHS (OCR) and NIST guidance and best practices.
    - Protective layered architecture framework from NSA, as DiD.
    - Risk assessment requirements and best practices from HIPAA security rules, DHHS (OCR), CMS, and NIST.
    - Selection decision support methods.
    - Risk assessment models and methods.

There are many qualitative and quantitative data points that firmly support the views of the participants impacted by the subjects of this research. The most significant examples of these key data points are the many regulatory requirements and impacts from non-compliance associated with the protection of ePHI and the question of who is accountable for that protection. These data were leveraged to perform an in-depth analysis of cases in which SMBE&A organizations with limited resources needed to select a risk assessment methodology and use it to determine risk levels for the ePHI that they process when facilitating patient care transactions within the cloud.

Research Participants

For this study, the researcher was the primary instrument for conducting, analyzing, and interpreting the research. The researcher reflected on how his role and personal background, culture, and experiences hold potential for forming his interpretations, such as the themes brought forward in this study and the impact of those themes on resolving the research questions.

Data Sources

The data collection for this study occurred in three phases. The initial phase consisted of research on vulnerabilities related to the rapid growth of IoT, the impact of those vulnerabilities on healthcare, specifically ePHI that is processed by SMB healthcare entities in the cloud, and the impacts of HIPAA compliance requirements on those healthcare entities. The second phase of data collection included research on risk assessment frameworks and methods that are best suited for SMB healthcare entities with limited resources and that process ePHI in the cloud. The third phase of data collection used the data collected in Phases One and Two, related to HIPAA compliance and best practice guidance from OCR and NIST, to develop a selection framework that includes criteria to aid with the selection of a best-fit risk assessment methodology for SMB healthcare entities. The third phase of data collection was conducted with framework instruments that included a decision matrix based on chosen selection criterion and a deployment example for the selected risk assessment methodology. For this study, a combination of qualitative and quantitative data helped to resolve the research questions.

Qualitative information. In the past, researchers "had to discuss the characteristics of qualitative research and convince faculty and audiences as to their legitimacy" (Creswell, 2014, pp. 201-202). While these discussions are now less frequent, it is critical to explain who participates in qualitative research and why their input is relevant and credible. The following information supports the use of qualitative methods for this study:

- *Researcher as key instrument:* The researcher for this study is a key research instrument and has over 30 years of experience in the field of Information Technology, which includes 20 years in various healthcare IT roles. In these roles, the researcher helped to lead numerous large-scale digital transformation initiatives

involving dozens of internal and external system integration architectures that are directly related to the subject area and problem statement for this study. These initiatives included:

- Design and implementation of Enterprise Application Integration Hub, such as a HIPAA validation engine that processed HIPAA validation of healthcare claims for over 3 million insured patients per year;
- Led architecture requirements for major system conversion from ICD-9 to ICD-10 codes – "ICD is International Statistical Classification of Diseases" (World Health Organization, 2018); and
- Led architecture requirements and design for a major system transformation with the goal of migrating the company from numerous and disparate on-premise, large scale mainframe and minicomputer systems to an external grouping of cloud-based systems with healthcare applications deployed with Software-as-a-Service models;
- Executive sponsor for a major initiative at SMBE&A to transform external integration hub by including more modern and standardized Application Programming Interfaces (APIs) that business partners can consume with a goal of reducing cost, risk, and complexity.

Toggle Magazine interviewed the researcher as a case study for his work as a CIO in the SMBE&A industry (Sulem, 2017). Given this broad and deep experience with healthcare IT, the researcher's background and experience suggest the credibility of the analysis and interpretations of the data being researched and of the findings presented.

- *Holistic account and reflexivity:* Researchers who use qualitative data to develop a comprehensive view of the problem being studied are said to be approaching their research with a holistic account. Qualitative researchers who use reflexivity to research qualitative data leverage documentation, observation of behaviors within the studied ecosystem, or interviews with participants in the study. For this study, reflexivity was leveraged by researching industry documents and observing behaviors that exist within the patient care ecosystem (Figure 7). Further information that supports using holistic accounts and reflexivity research approaches are described as follows.
    - Holistic account: This approach to research involves reporting multiple perspectives that arise across the field of study, identifying situational factors and explaining the broader picture that surfaces. For example, in Chapter 1, the ongoing increase in risks associated with the convergence of exponential growth of IoT and continued concerns over the privacy of personal information in the cloud were discussed. This study further refined the investigated population to SMBE&A that participate in patient care and use personal healthcare information. With a focus on SMB healthcare entities that have limited resources, this research then uses data around this focus area to develop criterion for selecting risk assessment methods.
    - Reflexivity: The researcher leveraged extensive research and surveys conducted in the Cost of Data Breach study by Ponemon (2016), which included 383 companies across 12 countries and had 63 U.S. companies participating. The surveys for these U.S. companies revealed that the US

leads all other global companies surveyed by 49% when considering data breaches that result in financial consequences. The cost of these breaches averages $3.97 million per incident and is mostly related to lost business. When healthcare-related factors associated with the value of patient data and the cost of HIPAA compliance are added, the cost continues to grow. Unmistakable evidence for HIPAA violations and HIPAA financial penalty settlements exist at the OCR Breach Portal, where researchers can confirm the IT assets breached, the number of individuals affected, and the healthcare entities involved. These data directly support the assertion that SMB healthcare entities are at a higher risk of exposing their ePHI due to technical vulnerabilities. When considered holistically, these datasets establish a foundation that helps to answer the research questions.

Quantitative information.

- *Surveys and research that include statistical information:* Surveys and scholarly research that included quantitative or numeric descriptions of trends were used to understand the attitudes and opinions of the healthcare industry regarding the vulnerability of ePHI when processed in a cloud by the SMBE&A population.
- *Regulatory requirements:* Research was conducted for this study to determine HIPAA requirements and the compliance and non-compliance costs of those requirements on SMBE&A. Further, HIPAA Security Rule requirements coupled with protective guidance from NIST and other sources were considered to assist with the development of criteria to be used to select an appropriate risk assessment model, as well as the factors to be considered to evaluate the risks of the selected model.

- *Decision-making processes and instrumentation:* A decision-making model was selected (a decision matrix) that included weighted numeric values to assist with a quantitative selection process for a risk assessment model to be used by the SMBE&A population.

Document analysis. The documents, artifacts, or sources critical to this study are coded below and logically grouped by theme, as shown in Table 3.

- DOCGRP01: Industry surveys, articles, reports, and scholarly research that confirm risks on the Internet for SMBE&A.
- DOCGRP02: HIPAA regulatory requirements and enforcement.
- DOCGRP03: OCR and NIST guidance and best practices for HIPAA compliance.
- DOCGRP04: Protective layered architecture framework from NSA, as DiD.
- DOCGRP05: Risk assessment requirements and best practices from HIPAA Security Rule, DHHS (OCR), CMS, and NIST.
- DOCGRP06: Risk assessment models and methods.
- DOCGRP07: Selection decision support methods.

Table 3. Document analysis table, by research theme group.

Research Theme Group	Document or Source Name
DOCGRP01	Enterprises Are Leading The Internet of Things Innovation (Afshar, V., 2017)
	Small, mid-sized businesses hit by 62% of all cyber attacks: Bad news: Financial services, including insurance, is on the most vulnerable list (Donlon, 2015)
	Healthcare Firms at Risk; Hackers Value Medical Records Over Credit Data (Humer, C., & Finkle, J., 2014)
	Prepare for Billions: The IoT 2020 IT Infrastructure Readiness Indicator (IDC, 2017)
	Hackers Selling Healthcare Data in the Black Market. (JA, A, 2015)
	The Internet of Things: 5 Predictions for 2018 (Kranz, 2018)
	4 reasons Cisco's IoT forecast is right, and 2 why it's wrong (Patterson, S., 2017)
	Uninvited Connections: A Study of Vulnerable Devices on the Internet of Things (IoT) (Patton, M., Gross, E., Chinn, R., Forbis, S., Walker, L., & Chen, H., 2014)
	2016 Cost of Data Breach Study: Global Analysis (Ponemon Institute, LLC, 2016)
	IoT devices being increasingly used for DDoS attacks: Malware is infesting a growing number of IoT devices, but their owners may be completely unaware of it (Symantec Security Response, 2016)
DOCGRP02	HIPAA Violations & Enforcement (American Medical Association, 2018)
	HIPAA Fines Listed by Year (Compliancy Group, 2018)
	Summary of the HIPAA Privacy Rule (DHHS Office for Civil Rights, 2013)
	Covered Entities and Business Associates (DHHS Office for Civil Rights, 2017)
	Cases Currently Under Investigation (DHHS Office for Civil Rights, 2018)
	EDI Resources: HIPAA (EDI Basics, 2018)
	Summary of the HIPAA Privacy Rule (DHHS Office for Civil Rights, 2013)
	Healthcare Information Privacy and Security: Regulatory Compliance and Data Security in the Age of Electronic Health Records (Robichau, B., 2014)
DOCGRP03	Addressing Gaps in Cybersecurity: OCR Releases Crosswalk Between HIPAA Security Rule and NIST Cybersecurity Framework (DHHS: Office for Civil Rights, 2016)
	Internet of Things (IoT) Cybersecurity Colloquium. A NIST Workshop Proceedings (Megas, K., Piccarreta, B., & O'Rourke, D., 2017)
	The NIST Definition of Cloud Computing: SP 800-145 (Mell, P., & Grance, T., 2011)
DOCGRP04	Defense in Depth (NSA, 2015)
	Protection of Information at Rest. NIST SP: Security and Privacy Controls for Federal Information Systems and Organizations (NIST, 2014)
	2010 Economic Analysis of Role-Based Access Control (O'Connor, A., & Loomis, R., 2010)
	Encryption of Cloud Data (Online Tech, LLC, 2013)
DOCGRP05	Basics of Security Risk Analysis and Risk Management (DHHS: Centers for Medicare & Medicaid Services, 2007)
	The Office of the National Coordinator for Health Information Technology (DHHS: ONC, 2014)
	Guide for Conducting Risk Assessments: SP 800-30, R1 (NIST: Joint Task Force for Transformation Inititative, 2012)
	Risk Management: Controlling Risk (Whitman, M., & Mattord, H., 2017)
DOCGRP06	Exiting the Risk Assessment Maze: A Meta-Survey (Gritzalis, D., Iseppi, G., Mylonas, A., & Stavrou, V., 2018)
	Choosing the right information security risk assessment framework (Mackey, R., 2011)
	The Quality Toolbox, Second Edition (Tague, N., 2004)
DOCGRP07	Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process (Caralli, R., Stevens, J., Young, L., & Wilson, W., 2007)
	Inventory of Risk Management / Risk Assessment Methods (ENISA, 2018)
	OWASP Risk Rating Methodology (OWASP, 2016)

Data Collection

As discussed in the data source section of Chapter 3, the researcher was the primary instrument for research throughout this study. As a result, data were collected through research and experience, as shown in Table 3. The data used to help answer the research questions were based on company and stakeholder surveys conducted across broad industry and geographical demographics that were refined to focus on the SMBE&A population in the U.S. The sources for these data included research organizations, analysts, publication authors, technology vendors, and scholars. These data sources include Cisco Systems, Ponemon Institute, IBM, global companies concerned with the impacts of data breaches, healthcare covered entities and business associates, U.S. Department of Health and Human Services (DHHS), DHHS Office of Civil Rights (OCR), Centers for Medicaid and Medicare Services (CMS), National Coordinator for Health Information Technology (ONC), Insurance Journals, National Institute of Standards & Technology (NIST), and several scholars from a variety of universities and research organizations.

Additional data were based on several layered requirements. The first was best practices and guidance for risk management frameworks and risk assessment and analysis capabilities. These data sources included the U.S. Department of Health and Human Services (DHHS), DHHS Office of Civil Rights (OCR), Centers for Medicaid and Medicare Services (CMS), National Coordinator for Health Information Technology (ONC), National Institute of Standards & Technology (NIST), European Union Agency for Network and Information Security (ENISA), and Open Web Application Security Project (OWASP).

The next set of data cane from DHHS, OCR, CMS, ONC, and NIST, which cooperate to provide guidance on HIPAA compliance requirements, best practices for implementing and maintaining

compliance, and explanations of the consequences that result from non-compliance. Finally, NIST, ENISA, and OWASP provide guidance, frameworks, and capabilities that can be used to assess ePHI vulnerabilities. In combination, these data sources were used as inputs for the development of a framework that SMB healthcare entities can use to select an appropriate risk assessment methodology to implement.

Data Analysis

For this data analysis, seven themes/categories of data (Table 3) were analyzed with the goals (a) confirming the assertion that ePHI is at risk when processed by SMB healthcare entities with limited resources and in the cloud and (b) using some of that same information to develop selection criterion to be used with a decision matrix to evaluate and select a best-fit risk assessment methodology. The sources that were leveraged to conduct this data analysis included industry surveys, regulatory publications and statistics, HIPAA compliance guidelines, and decision matrix modeling techniques and procedures. Table 4 lists each research question along with the applicable code(s) from Table 3 for the document analysis theme groups as well as a data analysis code that matches each research area with the appropriate research question and a consolidated definition with explanations and examples, where appropriate.

Table 4. Data analysis table.

Research Question	Document Analysis Code	Data Analysis Code
RQ1	DOCGRP01 & 02	DA-RA1
RQ2	DOCGRP02, 03, & 04	DA-RA2
RQ3	DOCGRP05 & 06	DA-RA3
RQ4	DOCGRP07	DA-RA4

DA-RA1. This data analysis method addresses RQ1 by considering research presented in Chapters 1 and 2 (DOCGRP01 & 02) regarding Internet growth and related vulnerabilities. This

analysis was done to justify the need to leverage an appropriate risk assessment model for SMBE&A. The data analysis evaluated and crosschecked appropriate data in DOCGRP01 & 02 to determine if risk related to SMBE&A that process ePHI transactions on cloud-based systems can be qualified. For example, Research from DOCGRP01 & 02 was used to first develop a predicted growth rate range for IoT. Multiple growth rate predictions were compared with variables that effected each growth rate to establish a refined range. More research was conducted and analyzed to determine what theoretical percentage of the refined IoT growth rate range includes vulnerable devices. Research was also conducted to determine the likelihood of an impact from the rapid growth of IoT on the U.S. healthcare industry on data (ePHI) breaches within the SMBE&A population.

DA-RA2. This data analysis method addresses RQ2 by considering research presented in Chapter 2 regarding HIPAA regulatory requirements and enforcement, along with guidance from NIST and NSA (DiD) that helped to identify related characteristics and risk factors that were later used in this study to evaluate, select, and utilize an appropriate risk assessment model for the SMBE&A population. The data analysis method conducted for DA-RA2 evaluated and cross-checked for appropriate data in DOCGRP02, 03, & 04 to determine the ideal characteristics and risk factors later used to create selection criteria for a risk assessment model that is a best fit for the SMBE&A population. For example, the definition of the SMBE&A population was established and its participation within the patient care ecosystem was illustrated (Figures 3 & 7). HIPAA regulatory and enforcement variables were also considered, as well as guidance for compliance from OCR, NIST, CMS, and NSA. Selection criteria, characteristics, and risk factors were derived from all appropriate data themes/groups (DOCGRP02, 03, & 04).

DA-RA3. This data analysis method addresses RQ3 by considering research presented in Chapter 2 that identified and evaluated those risk assessment models that are likely selection candidates for the SMBE&A population. The data analysis method conducted for DA-RA3 evaluated and crosschecked appropriate data in DOCGRP05 & 06 to determine a top three candidate list of risk assessment models that are likely good fits for the SMBE&A population. For example, research at the ENISA website and other sources revealed three selection candidates that are all aligned with at least multiple selection criteria (identified at DA-RA2). The top-three candidate list included Octave-S v1.0, ISO/IEC IS 13335-2, and Open Web Application Security Project (OWASP) Framework.

DA-RA4. This data analysis method addressed RQ4 by considering research presented in Chapter 2 that identified and demonstrated an effective decision matrix process that was later used in this study to evaluate and select a risk assessment model that is appropriate for the SMBE&A population. Further, the selected risk assessment model was tested with an example to illustrate its use by the SMBE&A population. The data analysis method conducted for DA-RA4 used data in DOCGRP07 to select a method and develop a decision matrix that was later used to select a best-fit risk assessment model from the top three candidate models that were identified in DA-RA3. The selected risk assessment model was then configured with the risk factors that were developed in DA-RA2. Further, a test risk assessment was completed with the configured model to provide an example of how the selected model can be used by the SMBE&A population to identify and evaluate risk levels for ePHI data that are processed on cloud-based systems.

Ethical Considerations

From the six key elements for ethical research set out in the ESRC Framework for Research Ethics (Economic and Social Research Council [ESRC], 2018), elements one, two, and six are relevant for this study:

- Element One - Research should be designed, reviewed, and undertaken to ensure integrity and quality. How did the researcher ensure quality and integrity for this study?
    - Answer One – The researcher ensured quality and integrity by using data from reputable sources and cross-checking them with similar sources.
- Element Two - Research staff and subjects must be fully informed about the purpose, methods, and intended possible uses of the research, what their participation in the research entails, and what risks, if any, are involved. Some variation is allowed in specific and exceptional research contexts for which detailed guidance is provided in the policy guidelines. Can the researcher ensure that any potential participants will be fully informed of the purpose, methods, and intended possible uses of the research?
    - Answer Two – As the researcher was the primary instrument for this study, the only other participants were indirectly involved as members of the thesis committee. All committee members were fully informed of the purpose, methods, and intended possible uses of the research.
- Element Six - The independence of the research must be clear, and any conflicts of interest or partiality must be made explicit. Will the research design enable the researchers to remain independent throughout the process? Are there any conflicts of interest?

- Answer Six – This study was conducted independently and did not raise or involve any conflicts of interest.

Summary of the Methodology

In this chapter, the philosophical worldview used in this study was introduced as pragmatism. The worldview was then refined to address points of view about ePHI vulnerabilities within the U.S. healthcare industry. Pragmatism was chosen because this study was based on actions, situations, and consequences related to vulnerabilities with ePHI processed by SMB healthcare entities with limited resources to protect patient information within cloud-based IT systems. This chapter also considered the various aspects of a hybrid qualitative and quantitative research design that was used for this study and included data collection and analysis approaches. In the next chapter, the findings that resulted from the research and analysis are discussed.

CHAPTER 4: FINDINGS

Introduction

The intention and objectives of this exploratory inquiry were to identify, assess, and reduce risks associated with the protection of ePHI that is processed in the cloud by SMB healthcare stakeholders and to do so in a way that is HIPAA compliant. The healthcare population studied for this research was a variety of healthcare covered entities and business associates (SMBE&A) involved a simple patient care scenario, as introduced in Chapter 2, that leverage various cloud-based resources.

Data collection for this hybrid qualitative and quantitative study occurred in three phases, with the initial phase consisting of research on vulnerabilities related to rapid growth of IoT and the impact of those vulnerabilities on ePHI that is processed by SMB healthcare entities in the cloud as related to HIPAA compliance requirements. The second phase of data collection included research on risk assessment frameworks and methods best suited to SMB healthcare entities with limited resources that process ePHI in the cloud. The third phase of data collection used the data collected in Phases One and Two, related to HIPAA compliance and best practice guidance from OCR and NIST, to develop a selection framework that includes selection criteria to aid with the selection of a best-fit risk assessment methodology for SMB healthcare entities. The third phase of data collection produced with framework instruments that include a decision matrix based on chosen selection criterion and an example deployed for the selected risk assessment methodology. For this study, the combined qualitative and quantitative data help to answer our research questions, which were introduced in Chapter 1:

RQ1: Does the risk of an ePHI breach justify the need to leverage a viable risk assessment model for the SMBE&A population?

RQ2: Through evaluation and assessment of HIPAA regulatory requirements and impacted IT architecture, what are the current *risk factors* for risk assessment that are critical for the SMBE&A population?

RQ3: Through evaluation and assessment of current risk models that meet HIPAA risk factor needs, what are candidate models for the SMBE&A population?

RQ4: What selection decision capability can be used by the SMBE&A population to evaluate and select an appropriate risk assessment model and how can the chosen model be leveraged to evaluate risk levels?

Interpretation

The results of the foregoing research are interpreted in this chapter through the thematic development of each research area.

Validity

Both the qualitative and quantitative data from surveys, statistics, case studies, and other evidence were verified and validated in this chapter through a thematic verification for each research area. For example, the research results from this study were used to connect and validate the qualitative data from surveys and use cases with quantified facts from scholarly research and breach investigations at the OCR HIPAA violations portal. According to Creswell (2014), "Validity is one of the strengths of qualitative research and is based on determining whether the findings are accurate from the standpoint of the researcher, the participant, or the readers of an account" (p. 201). Creswell also stated that "researchers must actively incorporate validity strategies into their thesis" (p. 201). There are eight primary strategies used to validate qualitative research. Following are the strategies employed for this research study:

- Triangulate different data sources of information by examining evidence from the sources and using it to build a coherent justification;
- use a rich, thick description to convey the findings, transport readers to the setting, and provide a discussion an element of shared experiences; and
- clarify the bias the researcher brings to the study to create an open and honest narrative that resonates with readers.

Results of Data Analysis

This section summarizes the analysis procedures used in this study to answer the research questions. Each research question is analyzed, and the results are given below in the form of research area narrative, themes, and theme verification.

DA-RA1. This data analysis addressed RQ1 by considering research presented in Chapters 1 and 2 (DOCGRP01 & 02) regarding rapid Internet growth and related vulnerabilities. This analysis was done to justify the need to leverage an appropriate risk assessment model for SMBE&A. The data analysis method included evaluating and cross-checking appropriate data in DOCGRP01 & 02 to determine if risk related to SMBE&A that process ePHI transactions on cloud-based systems can be qualified and quantified. RQ1 is resolved in this section of the study through thematic verification as follows.

Thematic development. When an aggregate view that included all data being analyzed for DA-RA1 was considered, themes that answered RQ1 developed. Those themes are as follows:

The impact of rapid IoT growth and unprotected IoT devices: When a rapid annual growth rate of 25% for IoT devices (Figure 1) is combined with a device vulnerability rate of 27%, we can see that rapid IoT growth is a catalyst for the acceleration of

breaches through unprotected IoT devices. We can no longer suggest that vulnerable devices on the Internet are rare. The time-series plot in Figure 13 shows that in 2017 there were over 28 billion IoT devices, of which 7.7 billion were vulnerable.

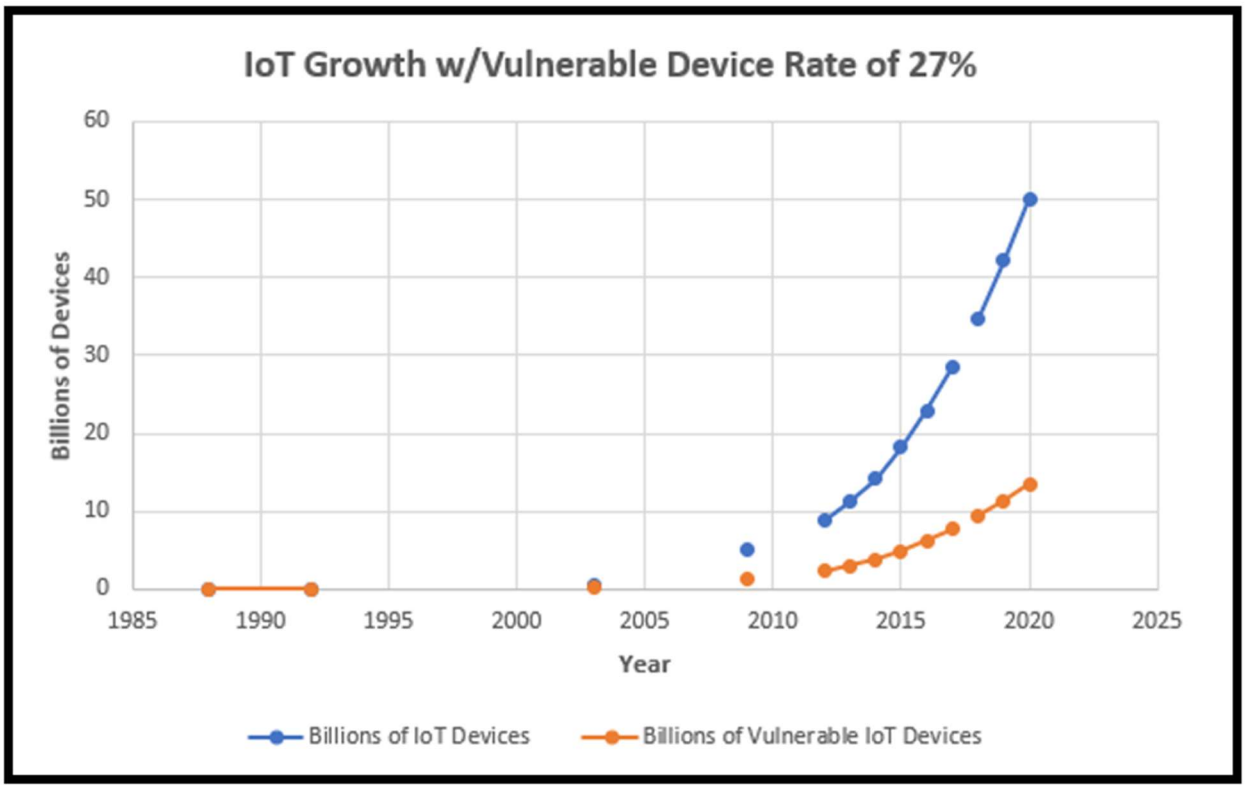

Figure 13. IoT vulnerable devices with 27% growth rate.

Risks and impacts associated with data breaches on the Internet: At 49% of global costs due to loss of business resulting from data breaches, the U.S. spent an average of $3.97 million per incident (Ponemon Institute, LLC, 2016). Contributors to the loss of business in the U.S. included loss of business reputation, costs of notification, and regulatory penalties. These data suggest that consumer perceptions of data privacy are clear drivers in the U.S of costs related to the loss of business that results from data breaches.

Impacts of data breaches resulting from HIPAA non-compliance: At $380 per capita, well above the mean of $225, healthcare companies lead in cost of losses per capita

across sixteen standard U.S. industry categories (Ponemon Institute, LLC, 2016). At 99.7%, SMB's represent a large majority of U.S. companies. However, if the average annual HIPAA settlement cost is $16M and all one hundred twenty-three covered entities under investigation are found to be non-compliant and to have had financial penalties enforced, that results in an average non-compliance cost of $133,000 (DHHS Office for Civil Rights [OCR], 2018). This indicates that HIPAA compliance costs are not a primary contributor to cost of data breaches in the healthcare industry.

Thematic verification. Positions revealed through thematic development were validated by understanding the relationships among statistical information.

- Cisco Systems predicted that, given its current rate of annual growth (25%), IoT will grow to 50 billion devices by 2020 (Afshar, 2017; Cisco 2013).
- Gartner, Inc., Hewlett-Packard, and IDC published more conservative predictions that would put IoT at 20-30 billion devices by 2020 (Gartner, Inc., 2015; IDC, 2017).
- The actual IoT growth rate lies in the hands of the consumers that drive IoT usage patterns. The more extreme IoT growth prediction of 50 billion devices by 2020 includes dependencies (Kranz, 2018) that will be catalysts for rapid IoT growth (25% annual growth rate). The combined research in DOCGRP01 & 02 suggested that there is an aggressive advancement of these dependencies, which could cause the more extreme growth prediction range to come to fruition. The dependencies include the following:
    - Artificial Intelligence (AI) will facilitate much faster IoT device onboarding;
    - Fog or Edge Computing is required for extreme IoT growth to be successful, and real time data processing must occur on the "edge" of the network; and

- blockchain is a basic requirement for highly regulated industries such as healthcare and finance.

The impact of rapid IoT growth on unprotected IoT devices:

- To validate the assumption that the IoT vulnerable device growth rate is 27%, the following data from DOCGRP01 & 02 were considered.
  - Number of devices on IoT in 2017: n = 28.4 billion;
  - Mean vulnerability rate: m = 27%;
    - SCADA Devices Scanned = .44%;
    - Traffic Control Devices Scanned = 40%;
    - Printers Scanned = 41%;
  - number of vulnerable devices scanned by Symantec every 2 minutes: = 7.7 billion.

The 27% growth rate for vulnerable IoT devices is depicted alongside general IoT growth rate in Figure 13.

Risks and impacts associated with data breaches on the Internet:

- Global increase in the total cost of data breaches since 2013 = 29%;
- U.S. increase in total cost of data breaches from 2014-2016 = 9%; and
- U.S. loss of business cost = $3.97 million per incident = 49% of global cost.

Impacts of data breaches resulting from HIPAA non-compliance:

- If 99.7% of U.S. companies are SMBs and 62% of those SMB companies are data breach victims, with 20% of those victims representing healthcare, then we can validate our assumption that the SMBE&A population is at risk of ePHI breaches.

- The 2017 Average HIPAA settlements cost of $16.4m / 123 possible entities fined equals $133,000 in cost per entity. This is evidence that financial penalties resulting from HIPAA non-compliance are not key contributors to loss of business for SMBE&A. Rather the reputational impacts, which include loss of business or other financial burdens, such as mitigation required to become compliant or correction from reputational damage, are the key sources of these losses.

Summary. When combined, the themes and the theme verification for DA-RA1 suggest that healthcare SMBs are at high risk of HIPAA data (ePHI) breaches and therefore must be equipped to assess and evaluate their company's risk levels with an appropriate risk assessment methodology and capability.

DA-RA2. This data analysis addresses RQ2 by considering research presented in Chapter 2 regarding HIPAA regulatory requirements and enforcement, along with guidance from NIST and NSA (DiD) that helped to identify related characteristics and risk factors used later in this study to select and utilize an appropriate risk assessment model for the SMBE&A population. The data analysis method conducted for DA-RA2 involved evaluating and cross-checked appropriate data in DOCGRP02, 03, & 04 to determine the ideal characteristics and risk factors used to create selection criteria for a risk assessment model that is a best fit for the SMBE&A population. RQ2 is resolved in this section of the study through a series of research area (RA2) themes and thematic verifications, as follows.

Thematic development. When an aggregate view that included all data being analyzed for DA-RA2 was considered, the following themes developed that answered RQ2:

Risk assessment requirements and capabilities: The research in Chapter 2 revealed that OCR and NIST developed a crosswalk table that maps NIST cybersecurity best practices

to HIPAA's privacy and security rules with the primary goal of "ensuring the confidentiality, integrity, and availability of electronic protected health information (ePHI) that covered healthcare entities and their business associates create, receive, maintain, or transmit" (DHHS: Office for Civil Rights, 2016, p. 3). Also revealed in Chapter 2 was that the "HIPAA Security Rule (HSR) requires health care providers, health plans, and business associates to conduct risk analyses and implement technical, physical, and administrative safeguards for ePHI (DHHS: Office for Civil Rights, 2016, p. 5)." One of the key HSR requirements that we are concerned with for this study is the requirement that all covered entities and business associates conduct risk analyses. Our research in this area revealed that CMS developed the HIPAA Security Series Papers, which included a paper focused on risk management called "Basics of Risk Analysis and Risk Management." This document aimed to connect HSR requirements with the risk assessment and management best practices published by NIST in SP 800-30. Because our selection criteria were only concerned with risk analysis capabilities, we included only the example risk analysis steps offered by CMS and NIST to help define our risk analysis capability selection criteria.

Development of selection criteria: Risk assessment model and capabilities should include specific assessment characteristics that are aligned with the needs of healthcare SMB entities that wish to understand their current risk posture regarding HIPAA non-compliance. Categories for these assessment characteristics include HSR requirements, SMB requirements, ability to estimate the likelihood of a breach, and ability to estimate the impact of a breach.

Thematic verification. Positions revealed through thematic development were verified and validated through evaluation of HIPAA regulatory requirements and impacted IT architectures. In addition, data were verified that were used to develop the final criteria for the selection of an appropriate risk assessment model for the SMBE&A population.

Risk assessment requirements and capabilities: The selection criteria should assist SMBE&A with the selection of a risk analysis model (RAM). Consultations that supported the development of the selection criterion included guidance from OCR and NIST per their crosswalk table (Table 1) and from the capabilities defined by CMS and NIST to facilitate risk analysis steps. A fully refined version of the OCR/NIST crosswalk table that was used to develop RAM selection criteria is provided in Table 5. Further, the standard risk analysis steps provided by CMS and NIST are provided as an additional

Table 5. OCR/NIST crosswalk table (fully-refined).

Function	Category	Subcategory	Relevant Controls	Relative Importance
IDENTIFY (ID)	Business Environment (ID.BE)	Company's role in supply chain	COBIT 5, NIST SP 800-53	Primary
	Governance (ID.GV)	Regulatory requirements	HIPAA Security Rule (HSR)	Primary
	Risk Assessment (ID.RA)	All Subcategories	COBIT 5, NIST SP 800-53, HSR	Primary
PROTECT (PR)	Access Control (PR.AC)	Identity mgt. established	COBIT 5, NIST SP 800-53, HSR	Primary
		Remote access managed	COBIT 5, NIST SP 800-53, HSR	Primary
		Access – Least privilege	NIST SP 800-53, HSR	Primary
	Awareness & Training (PR.AT)	Privileged users' roles/responsibility	COBIT 5, NIST SP 800-53, HSR	Primary
		Third-party roles/ responsibility	COBIT 5, NIST SP 800-53, HSR	Primary
	Data Security (PR.DS)	Data-at-rest is protected	CCS CSC 17, COBIT 5, NIST SP 800-53, HSR	Primary
		Data-in-transit is protected	CCS CSC 17, COBIT 5, NIST SP 800-53, HSR	Primary
		Protection continual improved	COBIT 5, NIST SP 800-53, HSR	Primary

resource to support further development of selection criteria for a RAM that is best suited to the SMBE&A population:

1. Identify the scope of the analysis,
2. gather data,
3. identify and document potential threats and vulnerabilities,

4. assess current security measures,
5. determine the likelihood of threat occurrence,
6. determine the potential impact of threat occurrence,
7. determine the level of risk, and
8. identify security measures and finalize documentation.

Development of selection criteria: The risk evaluation categories defined in Chapter 3 are used here to complete the development of selection criteria to be used within a chosen selection process or model, as defined in RA3. The final selection criteria are categorized and detailed as follows:

- ***HIPAA Security Rule Requirements (Business Needs and Impact)***

  Model flexibility – Risk assessment model must be flexible; consumers can customize and give high value to the impact of HIPAA non-compliance issues.

- ***SMB Characteristics***

  Low Cost – Most SMB healthcare organizations that process ePHI have limited resources to invest in high-cost risk assessment solutions.

  Low Complexity - Most SMB healthcare organizations that process ePHI have limited resources and skillsets required to effectively use and manage medium-to-highly complex risk assessment solutions.

- ***Estimating Likelihood***

  Threat – considers the worst-case threat agent, such as a hacker that is targeting specific data exploit opportunities.

  Vulnerability - Assuming a worst-case threat agent as the culprit, estimate the likelihood that stated vulnerability will be discovered and exploited.

- ***Estimating Impact***

  Technical Impact - To discover the depth and breadth of system or data impacts, technical impacts are considered to assess confidentiality, integrity, availability, and accountability.

  Business Impact – Consider the impact of system or data breaches on business operations, financial stability, reputation, and compliance concerns.

- ***Risk Assessment Capability Guidance***

  Regulatory Alignment – Most closely aligns with HIPAA Security Rule requirements and OCR/NIST guidance.

Summary. When combined, the themes and theme verification for DA-RA2 confirm the risk factors and selection criteria that were used in DA-RA3 to identify a top-three candidate list for risk assessment models that align with the needs of SMBE&A. Further, the selection criteria verified in DA-RA2 were used with a decision matrix model to evaluate and select the top three candidate risk assessment models.

DA-RA3. This data analysis addressed RQ3 by considering research presented in Chapter 2 that identified and evaluated those risk assessment models that are likely selection candidates for the SMBE&A population. The data analysis method conducted for DA-RA3 evaluated and crosschecked appropriate data in DOCGRP05 & 06 to determine a top three candidate list of risk assessment models that are likely good fits for the SMBE&A population. RQ3 is resolved in this section of the study through the following series of research area (RA3) themes and thematic verifications:

Thematic development. When an aggregate view that included all data being analyzed for DA-RA3 was considered, the following themes developed that answered RQ3:

Risk assessment requirements and capabilities: Research in Chapter 2 revealed that the "HIPAA Security Rule (HSR) requires health care providers, health plans, and business associates to conduct risk analyses and implement technical, physical, and administrative safeguards for ePHI" (DHHS: Office of Civil Rights, 2016, p. 5). The key HSR requirement that we have been concerned with in this study is the requirement that all covered entities and business associates conduct risk analyses. Our research in this area revealed that CMS developed the HIPAA Security Series Papers, which included a paper specifically focused on risk management called "Basics of Risk Analysis and Risk Management." This document aimed to connect HSR requirements with the risk assessment and management best practices published by NIST in SP 800-30. Its best practice guidance was leveraged in DA-RA3 to assist with discovering the top-three risk assessment models.

Broad characteristics considered when selecting candidate risk assessment models: As noted in Chapters 1 and 2, the SMBE&A population often has limited resources and knowledge required to identify and assess risks associated with ePHI vulnerabilities on cloud-based systems. Therefore, broad characteristics to consider when selecting candidate models include low cost, low complexity, easy access, and easy learning and deployment.

Thematic verification. Positions revealed through thematic development were verified and validated through the evaluation of current risk models that align with the following HIPAA risk factor and selection criteria:

Risk assessment requirements and capabilities: To establish a starting point for the discovery of models and methods, the study researched and leveraged the Inventory of

Risk Management and Risk Assessment Methods provided by the European Union Agency for Network and Information Security (European Union Agency for Network and Information Security [ENISA], 2018). ENISA is a center of expertise for cyber security in Europe. Due to the complexity of addressing cybersecurity across the diverse states of the European Union, this source was appropriate for considering the risk management methods used worldwide, and it also supports the research goals as they relate to HIPAA requirements. Risk assessment methods considered in this research and published by ENISA are as follows:

- Octave-S v1.0 for SMB's: The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE®) risk assessment model (Figure 10) was developed by the Software Engineering Institute of the Carnegie Mellon University. The U.S. Department of Defense first invested in this initiative to address HIPAA security standard compliance requirements.
- ISO/IEC IS 13335-2: An ISO standard describing the complete process of information security Risk Management in a generic manner. The annexes contain examples of information security risk assessment approaches as well as lists of possible threats, vulnerabilities, and security controls.
- Open Web Application Security Project (OWASP): An open community dedicated to enabling organizations to conceive of, develop, acquire, operate, and maintain applications that can be trusted (Open Web Application Security Project [OWASP], 2018).

Broad characteristics considered when selecting candidate risk assessment models:

- Octave-S v1.0 for SMB's: The U.S. Department of Defense was an early adopter of OCTAVE, which is used to address HIPAA compliance requirements. Octave-S is a subset of its traditional form and is tailored to fit smaller the business needs of smaller companies (less than 100 employees) (Caralli, Stevens, Young, & Wilson, 2007). While Octave-S appears to be available at no charge, it is "process-and-artifact-heavy," and its implementation information is dated (Alberts, Dorofee, Stevens, & Woody, 2005, p. 4).
- ISO/IEC IS 13335-2 can be understood as the basic information risk management standard at an international level, setting a framework for the definition of the risk management process. As previously discussed in this research, NIST SP 800-30, Revision 1 gives detailed guidance on identifying what should be considered within computer security risk management and risk assessment. Due to its broad use to address regulatory concerns, it is likely a good fit to address HIPAA requirements. However, it is a "process-and-artifact-heavy" solution intended for larger organizations.
- Open Web Application Security Project (OWASP): All OWASP tools, documents, forums, and chapters are free and open, making them an excellent choice for SMBs with limited resources. OWASP is governed worldwide by their foundational bylaws, core values, and code of ethics, which can all be reviewed at the OWASP website. The website includes templates and instructions (Petrak, 2015). An example of the OWASP risk assessment model is available in Figure 11.

Summary. When combined, the theme verification for DA-RA3 used the risk factors and selection criteria defined in DA-RA2 to identify a top three candidate list for risk assessment models that likely align with the needs of SMBE&A. All three of these candidate models align with HIPAA requirements and NIST guidelines. Further, all three candidate models align with one or more broad characteristics, which include low cost, low complexity, easy access, and ease with which the model can be learned and deployed.

DA-RA4. This data analysis addresses RQ4 by considering the research presented in Chapter 2 (DOCGRP07) that identified and demonstrated an effective decision matrix process that was used in this section of the study to evaluate and select a risk assessment model appropriate to the SMBE&A population. Further, the selected risk assessment model is provided as an example to illustrate possible use by the SMBE&A population. RQ4 is resolved in this section of the study through the following series of research area (RA4) themes and thematic verifications.

Thematic development. When an aggregate view that included all data being analyzed for DA-RA4 was considered, the following themes that answered RQ4 developed:

Using a decision matrix model as a decision support capability: The American Society for Quality (ASQ) has defined a Decision Matrix Model (DMM) as a framework that "allows teams to evaluate and prioritize a list of options. The team first establishes a list of weighted criteria and then evaluates each option against those criteria" (Tague, 2004). DMM populated with study-relevant and weighted criteria to support selection of risk assessment model: The simplest way to provide value to each criterion is to use broad, highly subjective ranking, as in 1, 2, 3 (1 = low, 2 = medium, 3 = high). More deliberate and less subjective approaches include applying weighted values to each criterion to

ensure that the most critical criteria are not over looked, or else something like the Pugh matrix can be used to evaluate new options against an established baseline, which may be one of the alternatives to the current product or service. For this study, our assumption was that SMBE&A are new to risk assessments and have not established a baseline. While this study did use weighted criteria, it did not include an established baseline.

Using DMM to select a risk assessment model: The decision matrix was populated using selection criteria that were developed throughout Chapter 2 and refined at DA-RA2 in Chapter 4.

Guiding by example with completed risk assessment, using selected model: After a risk assessment model was selected, a basic risk assessment was completed to illustrate its possible uses for the SMBE&A population.

Thematic verification. Positions revealed through thematic development were verified and validated in this section by illustrating the use of a DMM model to evaluate and select a best-fit risk assessment model for SMBE&A. Once a risk assessment model was selected, an example implementation of that chosen model was also provided.

Using a decision matrix model (DMM) as a decision support capability: A DMM was used to support the selection of a risk assessment model. A DMM template, illustrated in Table 6, is used in the following manner.

- Criteria are added along with their weighted values (W) across the top row.
- For each criteria-option combination, a rank (R) of 1-3 is input (3 = highest alignment, 2 = medium alignment, and 1 = low alignment).
- Multiply the R and W values for each criteria-option combination, (R x W) = combination score. Once scores have been determined for all criteria-option

combinations, add the combination scores for each solution option and input the total in the appropriate score total cell.

Table 6. Decision matrix template.

Weighted Criteria Solutions	Criteria-1 W = weighted value	Criteria-2 W = weighted value	Criteria-3 W = weighted value	Criteria-4 W = weighted value	Criteria-5 W = weighted value	Score Totals
Option 1	R = Rank (1-3) R x W = Score					Sum of all criteria scores
Option 2						
Option 3						

DMM populated with study-relevant criteria to support selection of risk assessment model: A list of risk factors and weighted criteria was established at DA-RA2 to be used with the DMM template and to support the selection of a risk assessment model.

Using DMM to select a risk assessment model: The list of risk factors and weighted criteria were added to the DMM template, the solution options were ranked and scored, and the selection was revealed (Table 7).

Table 7. Completed DMM for risk assessment model selection.

Weighted Criteria Solutions	Flexibility Weight = 4	Low Cost & Complexity Weight = 4	Threat & Vulnerability Weight = 2	Technical Impact Weight = 3	Business Impact Weight = 5	Score Totals
OCTAVE-S	**Rank = 2** (some custom) **W x R = 8**	**Rank = 2** (free, complex) **W x R = 8**	**Rank = 2** (some capability) **W x R = 4**	**Rank = 2** (some capability) **W x R = 6**	**Rank = 2** (some capability) **W x R = 10**	**36**
ISO/IEC IS 13335-2	**Rank = 1** (not custom) **W x R = 4**	**Rank = 1** (cost, complex) **W x R = 4**	**Rank = 3** (strong capability) **W x R = 6**	**Rank = 3** (strong capability) **W x R = 9**	**Rank = 1** (weak capability) **W x R = 5**	**28**
OWASP	**Rank = 3** (custom) **W x R = 12**	**Rank = 3** (free & easy) **W x R = 12**	**Rank = 1** (weak capability) **W x R = 2**	**Rank = 2** (some capability) **W x R = 6**	**Rank = 3** (strong capability) **W x R = 15**	**47**

Given the observations made during the research conducted in Chapter 2 and the results of the data analysis for DA-RA3, each solution option was ranked and scored, as follows:

- OCTAVE-S: (1) Flexibility – moderate with some customization possible; (2) Cost & Complexity – free, but moderately complex to implement; (3) Threat & Vulnerability – Moderate capability to setup this risk factor; (4) Technical Impact – Moderate capability to setup this risk factor; (5) Business Impact - Moderate capability to set up this risk factor.
- ISO/IEC 13335-2: (1) Flexibility – no customization possible; (2) Cost & Complexity – Moderate cost and difficult to implement; (3) Threat & Vulnerability – Strong capability to setup this risk factor; (4) Technical Impact – strong capability to set up this risk factor; (5) Business Impact – Weak capability to set up this risk factor.
- OWASP: (1) Flexibility – Highly customizable; (2) Cost & Complexity – free, low complexity to implement; (3) Threat & Vulnerability – Weak capability to

setup this risk factor; (4) Technical Impact – Moderate capability to setup this risk factor; (5) Business Impact – Strong capability to setup this risk factor.

Guiding by example with completed risk assessment using selected model: As the OWASP risk assessment model was selected, this study offered an example case for use of the model. The goal was to guide the SMBE&A population by example to encourage adoption of the model. The combination of Tables 8, 9, & 10 provides an example of a completed OWASP risk assessment for a patient care scenario, as depicted in Figure 7.

Table 8. Likelihood scores for OWASP example.

Likelihood								
Threat agent factors					Vulnerability factors			
Skill level	Motive	Opportunity	Size		Ease of discovery	Ease of exploit	Awareness	Intrusion detection
9 - Security penetration skills	9 - High reward	4 - Special access or resources required	9 - Anonymous Internet users		3 - Difficult	3 - Difficult	4 - Hidden	3 - Logged and reviewed
Overall likelihood:				5.500	MEDIUM			

Table 9. Impact scores for OWASP example.

	Technical Impact					Business Impact			
	Loss of confidentiality	Loss of integrity	Loss of availability	Loss of accountability		Financial damage	Reputation damage	Non-compliance	Privacy violation
Rating	5 - Extensive critical data disclosed	7 - Extensive seriously corrupt data	5 - Minimal primary services interrupted, extensive secondary services interrupted	7 - Possibly traceable		7 - Significant effect on annual profit	9 - Brand damage	7 - High profile violation	5 - Hundreds of people
Weight	40%	15%	15%	30%		20%	20%	25%	35%
Weighted Rating	2	1.05	0.75	2.1		1.4	1.8	1.75	1.75
	Overall technical impact:		5.900	MEDIUM		Overall business impact:		6.700	HIGH
	Overall impact:			6.300	HIGH				

Table 10. Overall risk severity level for OWASP example.

Overall Risk Severity = Likelihood x Impact				
Impact	HIGH	Medium	**High**	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

In the OWASP risk assessment example provided in Tables 8, 9, and 10, the following observations can be made.

- Overall likelihood rating – This rating was determined by evaluating all risk factors within the threat and vulnerability categories.
- Overall impact rating – This rating was determined by evaluating all impact factors within the technical and business impact categories.
- Overall risk severity level – For this example, the following observation was made:
    - The overall likelihood score was 5.5, which is considered a medium risk level by OWASP standards.
    - The overall impact score was 6.3, which is considered a high-risk level by OWASP standards.
    - When combined, the average for those risk levels is 5.9, which is considered a medium risk level by OWASP standards. However, because it is risk assessment best practice to give business risk priority over technical risk, the risk level has been rounded up to 6.0, which makes the overall risk severity level high. This is particularly important for this assessment, as the business risk factors that had high risk values were non-

compliance with HIPAA and privacy violation (ePHI at high risk of becoming compromised).

Summary. This data analysis addressed RQ4 by considering research presented in Chapter 2 (DOCGRP07) that identified and demonstrated an effective decision matrix process, which was used in this section of the study to evaluate and select a risk assessment model most appropriate for the SMBE&A population. Due to its flexibility, low cost and low complexity, and alignment to HIPAA requirements, the OWASP risk assessment model was selected. Further, the OWASP model was tested to illustrate its possible use for the SMBE&A population. RQ4 was resolved in this section of the study through a series of research area (RA4) themes and thematic verification.

Overall Results

With the data analysis themes herein revealed and verified, all four research questions have been answered and resolved. Chapter 5 provides a discussion of the results for all research analyses with the goal of revealing implications and recommendations for future research as well as for drawing conclusions.

CHAPTER 5: SUMMARY, IMPLICATIONS, CONCLUSIONS

Summary of Results and Discussion

In this chapter, a final summary of each of the four research areas is discussed to explain the implications of the results, to describe what gaps exist in current research, as to provide recommendations for future research.

Research Area One (RA1). To answer RQ1, this research area (RA1) included data analysis on the impact of vulnerabilities resulting from rapid IoT growth on ePHI data being processed by SMBE&A on cloud-based systems. Multiple data sources (DOCGRP01 & 02) were studied and crosschecked to determine if the risk level justified the need for SMBE&A to leverage a viable risk assessment model. The answer found was affirmative. Given recent increases in Internet usage patterns (Kranz, 2018), the Internet will continue to grow at a rate of 25% annually (Afshar, 2017), with vulnerabilities representing 27% of that growth. The study also found that healthcare patient records (ePHI) being processed by the SMBE&A population have the highest likelihood of being compromised and at the highest cost (Ponemon Institute, LLC, 2016). Given the clear target of ePHI by cybercriminals and the vulnerabilities of IoT, the SMBE&A population must leverage a viable risk assessment model to identify risk and determine severity levels so that they can plan for the mitigation of those risks.

Research Area Two (RA2). To answer RQ2, Research Area 2 (RA2) included research and data analysis on the characteristics of and risk factors related to HIPAA regulatory requirements (DHHS: Office for Civil Rights, 2013) and compliance guidance from NIST (NIST: Joint Task Force for Transformation Inititative, 2012) and the NSA (National Security Agency, 2015). These were later used to evaluate, select, and provide an implementation example (illustrative) of a best-fit risk assessment model for the SMBE&A population. To

accomplish this, many data sources (DOCGRP02, 03, & 04) were studied and crosschecked to determine which characteristics and risk factors were leveraged (DA-RA2). Those characteristics and risk factors were used to develop selection criteria that were later used to evaluate, select, and implement a risk assessment model for DA-RA3 and DA-RA4.

Research Area Three (RA3).

To answer RQ3, Research Area 3 (RA3) included research and data analysis (DOCGRP05 & 06) on risk assessment models that are likely selection candidates for the SMBE&A population. Using the criteria developed for DA-RA2, the following top-three candidate list was discovered and presented: OCTAVE-S, ISO/IEC IS 13335-2, and OWASP. Those selection candidates were further evaluated in RA4 to determine the best fit for the SMBE&A population.

Research Area Four (RA4).

To answer RQ4, Research Area (RA4) included research and data analysis (DOCGRP07) that identified, selected, and leveraged a selection decision support capability called a decision matrix. That decision matrix was then used to evaluate, score, and select a best fit risk assessment model for the SMBE&A population (DA-RA4). OWASP was selected based on its flexibility (highly customizable), low cost (free), low complexity (easy to access and implement), and strong ability to configure for and evaluate risk factors that included threat and vulnerability factors (to determine the likelihood of exploitation) and technical and business impacts (to determine the impact of exploitation) (Open Web Application Security Project, 2016). Further, the OWASP model was configured and explained by example with the goal of encouraging the SMBE&A population to adopt the OWASP model (Petrak, 2015).

Implications

The findings of this study contributed knowledge to the field of information security, the healthcare industry, and the combined industry of Health IT (HIT). More specifically, as 62% of cyber-breach victims are SMB companies, SMBE&A with limited resources should leverage this research to assess risk severity levels for the ePHI data that they process, and this can be achieved with low effort, at low cost, with low complexity, and with high flexibility. These findings were enabled through the capture and analysis of industry surveys, industry statistics, existing scholarly research and analysis, HIPAA requirements for the protection of ePHI, information security best practices and guidance from NIST and NSA, and the risk assessment framework and rating practices from the OWASP.

While the benefits and contributions to healthcare IT from this research are many, the researcher did observe some gaps. For example, many SMBE&A are very small. Those in start-up status have very limited IT or financial resources and may not even be aware of their responsibilities when processing ePHI. Where do these companies go for help? How will they know if they need help? Another gap is the wide variation in how SMBE&A integrate and exchange information with one another. If these companies cannot account for the successful delivery of ePHI transaction payloads, how can they ensure that data privacy and integrity have been accomplished? As explained in the recommendations section of this chapter, there are also many emerging regulations and protective capabilities on the horizon that must be considered. What can be leveraged from those opportunities to improve the protection of ePHI data going forward?

Recommendations for Future Research

As indicated in the implications section of this chapter, several gaps that need to be considered going forward. This section will suggest recommendations for addressing those gaps.

Recommendation one. For SMBE&A that have limited IT or financial resources, research could be conducted that considers maturation opportunities for these companies in the field of healthcare IT and information security in the context of HIPPA compliance. Like the way that the crosswalk table was implemented, OCR and NIST could further their work to include compliance "starter kits," along with assessments, tests, and certifications that result in full compliance for SMBE&A organizations. Research should also be conducted to determine the feasibility of including the OWASP risk assessment framework in the compliance starter kit. Further, SMBE&A with a record of accomplishment in compliance certification could become integration hubs of excellence that help to set standards for less mature entities. Along with compliance, these companies can benefit from consolidation of otherwise disparate transaction processing, improving their industry footprint as a certified healthcare integrator as a result.

Recommendation two. Related to recommendation one, future research should consider improvements in API standardization and management for SMBE&A. While APIs have been in use for many years, the variations with which APIs are deployed are very broad. This variation in approach will be further expanded because of the rapid the IoT growth discussed throughout this study. According to Gartner analysts, "the cost of application integration is approximately 30% more than the cost of the applications being integrated" (O'Neill, Malinverno, & Biscotti, 2017, p. 3). Much of this cost is due to poor integration techniques and integration implementations that must be rebuilt because of improper initial builds. The Gartner analysts further predicted that, "By 2021, 65% of new applications will be built as a mesh of multichannel

apps and multi-grained back-end services that communicate via APIs" (O'Neill, Malinverno, & Biscotti, 2017, p 4). The Garter study proposed that a forum be created to help facilitate API standardization and management as well as centers of integration excellence for SMBE&A.

Recommendation three. With emerging regulatory requirements like GDPR, all global companies are at risk of severe financial penalties or loss of business because of non-compliance. "GDPR" stands for General Data Protection Regulation and seeks to create a data protection regulatory framework across the European Union (EU) with the goal of returning control of personal data to citizens. GDPR requirements are not unique to only the EU; strict rules will be imposed on those hosting and processing these personal data anywhere in the world. For example, global companies that process any data that belongs to an EU citizen are required to "implement appropriate technical and organizational measures, by May 25th, 2018" (Yelland, 2017, p. 2). While many U.S. companies may feel that they are immune to this EU regulation, global U.S. companies are absolutely in scope, and it is only a matter of time before similar regulations will be implemented in the U.S. With U.S. healthcare becoming even more expensive because of cybercrime, this kind of regulatory change is inevitable. All U.S. companies—small, medium, and large—should start preparing now. Many emerging capabilities will likely expand the risk mitigation options associated with breaches of ePHI data. For example, more extensive research and testing should be conducted on using capabilities like Blockchain, IDPS, DLP systems that leverage AI capabilities, and Cyber Insurance. In combination, research on and advancement of these protective capabilities could provide more automated and predictive protective capabilities and reduce the strain on resource-constrained companies like those in the SMBE&A population.

Conclusion

According to the research in this study and many others, as well as the nightly news, the probability of data breaches is high. This study investigated how to best assess risks related to ePHI data that is processed in the cloud. More specifically, this study conducted research on reducing risk for SMBE&A that process ePHI data in the cloud. Using a hybrid research design, we used qualitative and quantitative data to answer research questions related to justification for the research, developing a common understanding of the characteristics of vulnerability for ePHI data, and risk assessment options that can be leveraged to aid with HIPAA compliance. We then leveraged that research to answer additional research questions around determining risk severity levels for ePHI transactions that originate within the SMBE&A population. However, it was observed that SMBE&A must consider all related factors when evaluating risk, which are sometimes ancillary and not obvious. In the case of our OWASP implementation example, the outlier risk severity level of high was due to the high-risk ratings for business impact factors related to HIPAA non-compliance and privacy breaches (i.e., a high risk of ePHI data becoming compromised). A breach of this type would likely result in significant financial, reputational, and compliance issues. Therefore, this study found that SMBE&A personnel cannot analyze ePHI transactions in isolation.

The research throughout this study produced numerous examples of both qualitative and quantitative information that clearly and consistently justified our need to conduct deeper research to support identifying and assessing risks associated with ePHI vulnerabilities on cloud-based assets and when SMBE&A are liable. The information that supported the reliability and validity for the answers to the research questions in this study included industry surveys, case studies, HIPAA regulatory compliance requirements, and non-compliance violation outcomes

and examples that have been published and endorsed by the U.S. Department of Health and Human Services.

As discussed in the "Recommendations for Future Research" section of this chapter, there are many emerging opportunities to improve the ways that we assess and mitigate the risks associated with ePHI. Those opportunities range from improvements in HIPAA compliance guidelines from OCR and NIST with a focus on compliance starter kits for SMBE&A with limited resources to leveraging emerging capabilities such as Blockchain, IDPS, and DLP systems that use AI capabilities and Cyber Insurance. Since cybercrime is here to stay, it will be critical to remain focused on the protection of ePHI and all confidential information as it moves throughout the cloud-based patient care ecosystem.

REFERENCES

Afshar, V. (2017). *Cisco: Enterprises Are Leading The Internet of Things Innovation.* Chicago: Huffington Post: Huffpost News.

Alberts, C., Dorofee, A., Stevens, J., & Woody, C. (2005). OCTAVE®-S Implementation Guide, Version 1.0. In C. Alberts, A. Dorofee, J. Stevens, & C. Woody, *Volume 1: Introduction to OCTAVE-S* (pp. 5-6, 8). Pittsburgh: Carnagie Mellon: Software Engineering Institute.

American Medical Association. (2018, March 21). *HIPAA Violations & Enforcement*. Retrieved from AMA Practice Management: HIPAA Compliance: https://www.ama-assn.org/practice-management/hipaa-violations-enforcement

Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process.* Pittsburgh: Carnegie Mellon: Software Engineering Institute.

Cisco Systems, Inc. (2015). *Fog Computing and the Internet of Things: Extend the Cloud to Where the Things Are.* San Jose: Cisco Systems, Inc.

Compliancy Group. (2018, February 14). *HIPAA Fines Listed by Year*. Retrieved from Compliancy Group: https://compliancy-group.com/hipaa-fines-directory-year/

Covey, S. (1989). *The 7 Habits of Highly Effective People.* New York: Touchstone.

Creswell, J. W. (2014). Research Questions and Hypotheses. In J. W. Creswell, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (p. 148). London: SAGE Publications, Inc.

DHHS Office for Civil Rights (OCR). (2018, January 1). *Cases Currently Under Investigation*. Retrieved from OCR Breach Portal: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

DHHS Office for Civil Rights. (2013, July 26). *Summary of the HIPAA Privacy Rule*. Retrieved from HHS.gov: Health Information Privacy: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

DHHS Office for Civil Rights. (2017, June 16). *Covered Entities and Business Associates*. Retrieved from HHS.gov: Health Information Privacy: https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html

DHHS: Centers for Medicare & Medicaid Services. (2007, March 1). *Basics of Security Risk Analysis and Risk Management.* Retrieved from DHHS CMS: HIPAA Security Series: https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf

DHHS: Office for Civil Rights. (2016, February 23). *Addressing Gaps in Cybersecurity: OCR Releases Crosswalk Between HIPAA Security Rule and NIST Cybersecurity Framework*. Retrieved from HHS.gov: Health Information Privacy: https://www.hhs.gov/hipaa/for-professionals/security/nist-security-hipaa-crosswalk/index.html

DHHS: ONC. (2014, March 30). *The Office of the National Coordinator for Health Information Technology (ONC).* Retrieved from healthit.gov: https://www.healthit.gov/sites/default/files/risk_assessment_user_guide_final_3_26_2014.pdf

Donlon, R. (2015, May 27). Small, mid-sized businesses hit by 62% of all cyber attacks: Bad news: Financial services, including insurance, is on the most vulnerable list. *Property Casualty 360*, pp. 1-3.

Economic and Social Research Council (ESRC). (2018, June 16). *Key Ethics Principles*. Retrieved from The Research Ethics Guidebook: A Resource for Social Scientists: http://ethicsguidebook.ac.uk/Key-ethics-principles-15

EDI Basics. (2018, January 30). *EDI Resources: HIPAA*. Retrieved from EDI Basics: Your Resource for Learning About EDI: https://www.edibasics.com/edi-resources/document-standards/hipaa/

European Union Agency for Network and Information Security (ENISA). (2018, March 23). *Inventory of Risk Management / Risk Assessment Methods* . Retrieved from ENISA: RM/RA Methods: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods

Farahmond, F. (2010). Risk Perception and Trust in Cloud. *ISACA Journal*, 1-7.

Gartner, Inc. (2015). *Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015.* Stamford: Gartner, Inc.

Gartner, Inc. (2018, March 21). *IT Glossary: Small and Midsize Business (SMB)*. Retrieved from Gartner: https://www.gartner.com/it-glossary/smbs-small-and-midsize-businesses/

Gritzalis, D., Iseppi, G., Mylonas, A., & Stavrou, V. (2018). Exiting the Risk Assessment Maze: A Meta-Survey. *Association for Computing Machinery: ACM Computing Surveys*, 1-28.

HealthInsurance.org. (2018, March 21). *What is an explanation of benefits?* Retrieved from Glossary: Explanation of Benefits: https://www.healthinsurance.org/glossary/explanation-of-benefits/

Humer, C., & Finkle, J. (2014, September 24). Healthcare Firms at Risk; Hackers Value Medical Records Over Credit Data. *Insurance Journal*, 1-2.

IDC. (2017). *Prepare for Billions: The IoT 2020 IT Infrastructure Readiness Indicator.* Framingham: International Data Corporation (IDC).

JA, A. (2015). *Hackers Selling Healthcare Data in the Black Market.* Chicago: Infosec Institute.

Jones, E. (2014, September 1). *HIPAA "Protected Health Information": What Does PHI Include?* Retrieved from HIPAA.com: https://www.hipaa.com/hipaa-protected-health-information-what-does-phi-include/

Kranz, M. (2018, January 25). *The Internet of Things: 5 Predictions for 2018*. Retrieved from Cisco Blogs: https://blogs.cisco.com/innovation/the-internet-of-things-5-predictions-for-2018

Mackey, R. E. (2011). *Choosing the right information security risk assessment framework.* Newton: TechTarget.

Megas, K., Piccarreta, B., & O'Rourke, D. G. (2017). Internet of Things (IoT) Cybersecurity Colloquium. *A NIST Workshop Proceedings* (p. 3). Gaithersburg: National Institute of Standards and Technology.

Mell, P., & Grance, T. (2011, September 1). *The NIST Definition of Cloud Computing: SP 800-145.* Retrieved from NIST: Computer Security Resource Center: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Merriam-Webster, Incorporated. (2108). *Merriam-Webster Dictionary.* Springfield: Merriam-Webster.

National Security Agency. (2015, July 16). *Defense in Depth.* Retrieved from Information Assurance: By the National Security Agency: https://www.iad.gov/iad/library/ia-guidance/archive/defense-in-depth.cfm

Newman, D. (2017, September 26). *Top 10 Trends For Digital Transformation In 2018*. Retrieved from Forbes: CMO Network: #Getting Buzz: https://www.forbes.com/sites/danielnewman/2017/09/26/top-10-trends-for-digital-transformation-in-2018/#3f5e0e52293a

NIST. (2014). Protection of Information at Rest. *NIST SP: Security and Privacy Controls for Federal Information Systems and Organizations*, F-203.

NIST: Joint Task Force for Transformation Inititative. (2012). *Guide for Conducting Risk Assessments: SP 800-30, R1.* Gaithersburg: National Institute of Standards and Technology.

O'Connor, A. C., & Loomis, R. J. (2010). *2010 Economic Analysis of Role-Based Access Control.* Gaithersburg: NIST and Research Triangle Institute.

Office for Civil Rights (OCR). (2003, May 1). *Summary of the HIPAA Privacy Rule.* Retrieved from United States Department of Health and Human Services (DHHS): https://www.hhs.gov/sites/default/files/privacysummary.pdf

Office of the National Coordinator for Health Information Technology (ONC), DHHS Office for Civil Rights (OCR), & DHHS Office of the General Counsel (OGC). (2017, March 13). *HealthIT.gov*. Retrieved from Security Risk Assessment: https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment

O'Neill, M., Malinverno, P., & Biscotti, F. (2017). *Emerging Technology Analysis: Full Life Cycle API Management.* Stamford: Gartner Research.

Online Tech, LLC. (2013). *Encryption of Cloud Data.* Ann Arbor: Online Tech, LLC.

Open Web Application Security Project (OWASP). (2018, January 22). *Welcome to OWASP*. Retrieved from owasp.org: https://www.owasp.org/index.php/Main_Page

Open Web Application Security Project. (2016, May 30). *OWASP Risk Rating Methodology*. Retrieved from owasp.org: https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

Patterson, S. M. (2017, April 25). 4 reasons Cisco's IoT forecast is right, and 2 why it's wrong. *NetworkWorld: IoT Connected Intelligences*, pp. 1-4.

Patton, M., Gross, E., Chinn, R., Forbis, S., Walker, L., & Chen, H. (2014). Uninvited Connections: A Study of Vulnerable Devices on the Internet of Things (IoT). *IEEE Computer Society, IEEE Joint Intelligence and Security Informatics Conference* (pp. 232-235). The Hague: IEEE.

Pemberton-Levy, H. (2016). *The CIO's Guide to Blockchain.* Stamford: Gartner, Inc.

Petrak, H. (2015, May 31). *OWASP Risk Rating Template (Excel format)*. Retrieved from OWASP: https://www.owasp.org/images/5/5b/OWASP_Risk_Rating_Template_Example.xlsx

Ponemon Institute, LLC. (2016). *2016 Cost of Data Breach Study: Global Analysis.* Traverse City: Ponemon Institute: Research Reports.

Rice, C. (2002, September 8). CNN LAte Addition with Wolf Blitzer. (W. Blitzer, Interviewer)

Robichau, B. P. (2014). *Healthcare Information Privacy and Security: Regulatory Compliance and Data Security in the Age of Electronic Health Records.* Berkley: Apress.

Souppaya, M., & Scarfone, K. (2016). *User's Guide to Telework and Bring Your Own Device (BYOD) Security.* Gaithersburg: NIST.

Sulem, M. (2017, December 21). *Brett Luna - Healthesystems: Get Back to Work.* Retrieved from Toggle Magazine: https://www.togglemag.com/case-studies/brett-luna-healthesystems/

Symantec Security Response. (2016). *IoT devices being increasingly used for DDoS attacks: Malware is infesting a growing number of IoT devices, but their owners may be completely unaware of it.* Sunnyvale: Symantec Corporation.

Tague, N. R. (2004). Decision Matrix. In N. R. Tague, *The Quality Toolbox, Second Edition* (pp. 219-223). Milwaukee: American Society for Quality, Quality Press.

The Consumer Goods Forum; Capgemini; Intel. (2016). *Making the Connection: How the Internet of Things Engages Consumers and Benefits Business.* Santa Clara: Intel Corporation.

U.S. Department of Homeland Security (DHS). (2018, May 31). *Combating Cyber Crime*. Retrieved from Homeland Security: Cybersecurity: https://www.dhs.gov/topic/combating-cyber-crime

Wagner, D. (2018, January 14). *Goodreads Author: Daniel Wagner*. Retrieved from Goodreads: https://www.goodreads.com/author/show/15463683.Daniel_Wagner

Westerman, G., Bonnet, D., & McAfee, A. (2014). The Nine Elements of Digital Transformation. *MIT Sloan Management Review*, 1-3.

Whitman, M. E., & Mattord, H. J. (2017). Risk Management: Controlling Risk. In M. E. Whitman, & H. J. Mattord, *Management of Information Security* (p. 308). Boston: Cengage Learning.

World Health Organization. (2018, February 23). *Classification of Diseases (ICD)*. Retrieved from who.int: http://www.who.int/classifications/icd/en/

Yelland, B. (2017). *GDPR: How it Works.* United States: IBM.

Yilmaz, K. (2013). Comparison of quantitative and qualitative research traditions: Epistemological, theoretical, and methodological differences. *European Journal of Education*, 311-325.