11-2016

Is Cloud Computing in Healthcare Providing a Safe Environment for Storing Protected Health Information? A Systematic Review and Meta-Analysis

Ashley N. Hayes
University of Tennessee Health Science Center

Is Cloud Computing in Healthcare Providing a Safe Environment for Storing Protected Health Information? A Systematic Review and Meta-Analysis

Ashley N. Hayes

Entry-Level Masters

Advisor: Dr. Sajeesh Kumar

Health Informatics Information Management

University of Tennessee Health Science Center

November 3, 2016

Acknowledgements

I would like to thank all of the HIIM faculty at UTHSC for teaching me how to become a HIIM professional. Thank you to Dr. Rebecca Reynolds, Dr. Marcia Sharp, Dr. Beth Bowman, and Dr. Sajeesh Kumar for their guidance throughout my time in the program. Most importantly, I would like to thank my family for their encouragement and everlasting support.

This thesis is dedicated to my daughter, Avery. When she is old enough to understand, I hope she will see that hard work and dedication to a higher education can provide a lifetime of opportunities. I also want her to learn that no matter how hard, or how long the path may be, you should never give up on your goals.

Abstract

Over the past several years, cloud computing has become increasingly more popular for the use of storing, accessing, and maintaining electronic health records (EHRs). In comparison to conventional EHR management tools, such as installed software, cloud computing offers more capabilities for medical facilities and their patients. Experts claim that in addition to changing the face of health information technology, it will also advance healthcare services, and benefit medical research. As the use of cloud computing has increased, so has the amount of healthcare data breaches. This study is proposing that there is a correlation between the increase in cloud computing protected health information (PHI), and healthcare data breaches. This study researches the top five largest healthcare data breaches in 2015 what the organizations' could have done differently. This study also proposes that current privacy and security laws do not clearly defined cloud computing regulations. Suggestions are also made for organizations to employ a multilevel security framework for cloud-based applications. This information will be valuable to all health information management (HIM) professionals that are involved in migrating and maintaining PHI stored in the cloud.

Keywords: cloud computing, electronic health record (EHR), protected health information (PHI), privacy, security

Table of Contents

List of Tables

List of Figures

Privacy and Security Issues with Cloud Computing Protected Health Information

Chapter 1

Introduction

The National Institute for Standards and Technology (NIST) defines cloud computing as "a model for enabling 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." (Dinh, 2011, p. 36). Cloud computing is increasingly becoming the preferred choice by many healthcare organizations for the management of their EHR systems. The main advantages of cloud based EHRs is the ability to share patient information with other clinicians inside and outside of the organization, the ability to store all records in one place, and the ability to access records from any location at any time. The advantage of on-demand access is also extended to patients. Cloud based EHRs allow patients to access, duplicate, and transfer their own protected health information (PHI).

The Health Insurance Portability and Accountability Act (HIPAA) of 1996, the Department of Health and Human Services (HHS) developed the HIPAA Privacy Rule and Security Rule. The Privacy Rule established national standards to protect certain health information. This rule requires healthcare organizations, also known as "covered entities", to allow patient health records to be available for the purpose of medical treatments, either through a court order or through signed patient consent. Patients must be notified of the use of their PHI by the organization. The Security Rule elaborates on the Privacy Rule by establishing national standards for protecting PHI created, maintained, and stored in electronic formats. Organizations

must guarantee security of administrative, technical, and physical safeguards, while also ensuring the confidentiality, integrity, and availability of PHI (Rodrigues, 2013).

With benefits such as reduction of costs, increased efficiencies, and flexibility, it is clear why more organizations are transitioning to cloud based applications, as opposed to conventional systems. Unfortunately, there are many privacy and security issues that healthcare professionals, and their patients should be aware of. The purpose of this paper is to discuss these issues that exist from cloud computing confidential health information, and determine if information stored in the cloud is safe. This paper will cover the significance of cloud computing health information, the privacy and security concerns that result from storing confidential data in the cloud, the different types of cloud structures, and the effectiveness of various security mechanisms.

Background

Even though cloud computing is relatively new to the healthcare industry, the technology has been available for many years. Examples of commonly used cloud services include Google Docs and Picasa. These two examples are free to the public and allow users to easily upload documents or pictures from their computer or mobile devices. It is called the cloud because it is described as a virtual cloud in the sky, which depending on its design, can contain servers, applications, databases, and space for storing files. Once documents are uploaded to the cloud, they can be retrieved from any location via an internet connection and proper login credentials. Cloud computing in healthcare consists of more intricacies and serves a variety of other purposes than the examples above. Organizations may decide to adopt cloud based technology in order to reduce maintenance and storage costs, increase storage capabilities, facilitate health information exchange, and on-demand access to information from any location. Depending on the

organization and their needs, there are different types of service models infrastructure-as-a-service (IaaS), service-as-a-structure (SaaS), and platform-as-a-service (PaaS). There are four different types of delivery models: public, private, hybrid, and community. The service and delivery models are investigated in this paper to determine any differences in security levels.

Purpose of the Study

The purpose of this study to evaluate the privacy and security of protected health information (PHI) when healthcare organizations use cloud computing technologies to store, maintain, and communicate personally identifiable information. Through systematic review, this study attempts to find a correlation between the use of cloud computing technology and the recent increase in healthcare data breaches. This study investigates four studies conducted on the use of cloud based services and data breaches in healthcare.

Significance of the Study

This study aims to further educate HIM professionals on the privacy and security issues on cloud computing PII and PHI. As the amount of medical information increases, so has the adoption of cloud computing technologies. Cloud computing allows organizations the flexibility of virtualization by storing and maintaining larger amounts of information without the need for physical storage space. There are many educational resources available on the benefits and challenges associated with cloud computing, but few studies have focused on the impacts that cloud computing has on the security of health information.

HIM professionals will benefit from this study by gaining a better perspective of the possible outcomes that result from an electronic data breach. Data breaches to PHI stored in the cloud occur because of a lack of employing preventative measures. Through this study, HIM professionals are able to Some organizations remain hesitant to transition their health records to

the cloud because of a lack of industry standards, and the fear of not only to the affected individual patients, but also to the organization, and the healthcare industry as a whole.

Research Questions

This study is intended to determine if the increase healthcare data breaches is attributed to the increased adoption of cloud computing technologies. This study aims to answer the following three questions:

- How much have healthcare data breaches increased since the widespread adoption of cloud based services?
- Is the increase in data breaches directly related to the use of cloud based services?
- Is personally identifiable information (PII) and PHI stored in the cloud secure?

Definition of Key Terms

- Cloud Computing- a model for enabling 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 (Dinh, 2011, p. 36).
- Business Associates- third party contract vendors, such as cloud services providers.
- Data breach- An impermissible use or disclosure that compromises the privacy or security of protected health information.
- HIPAA- Health Insurance Portability and Accountability Act of 1996; Federal law enacted giving patients the right to access their health information at any time and the right to share their information with whomever they choose.

- HIPAA Privacy Rule- Requires appropriate safeguards to protect the privacy of personal health information, and limits the use of and disclosure of such information without prior authorization from the patient.
- HIPAA Security Rule- Requires covered entities to employ appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and security of confidential health information is that electronically created, received, used, stored, and maintained by the entity
- HITECH Act- Health Information Technology for Economic and Clinical Health Act of 2009; Enacted as part of the American Recovery and Reinvestment Act of 2009 to help encourage the adoption and meaningful use of health information technology. Helps to strengthen the HIPAA Privacy Rule and Security Rule (U.S. Department of Health & Human Services, 2016).
- Hybrid Cloud- Deployment model consisting of two or more deployment models combined.
- IaaS- Infrastructure-as-a-service; Service model that serves as a foundation for other service models. The healthcare organization does not manage or control the cloud infrastructure, but they do have control over operating systems, storage, applications, and limited control of select networking components.
- PaaS- Platform-as-a-service; the healthcare organization is able to create and modify applications that run on the cloud service provider's environment (Goyal, 2014).
- PHI- Protected health information; individually identifiable health information that is created or maintained by a covered entity and any business associates acting for the

covered entity (U.S. Department of Health and Human Services National Institutes of Health, 2007).

- PII- Personally identifiable information; "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information" (McCallister, 2010, p. 7).
- Privacy- Individuals' right to protect their personal information from being observed or damaged by other people.
- Private Cloud- Cloud deployment model that is designed and operated specifically for an organization. Only members of that organization have access to the cloud.
- Public Cloud- Cloud deployment model that is owned a third party cloud service provider and is available to the public. Resources are offered as services for a pay-for-usage fee (Goyal, 2014).
- Security- Individuals' rights to have their personal information protected and safe from unwanted access by others and free of harm.
- SaaS- Software-as-a-service; cloud service model where the organization uses the cloud service provider's applications (Goyal, 2014).

Chapter 2

Review of Literature

Findings

Significance of Cloud Computing in Healthcare. Since the American Recovery and Reinvestment Act of 2009 (ARRA) included the Health Information Technology for Economic and Clinical Health (HITECH) Act, the adoption of cloud based storage has rapidly increased. The HITECH Act prompted the Department of Health and Human Services (HHS) to develop the Meaningful Use program that offers eligible professionals, eligible hospitals, and critical access hospitals (CAHs) incentive payments for meeting objectives required by the Centers for Medicare and Medicaid Services (CMS). In order to meet Stage 2 objectives, healthcare providers must allow patients to view, download, and transmit their health information. For hospitals, patients must have access within 36 hours of discharge, and eligible professionals must do so within four business days. In order to provide this access, many organizations are turning to cloud based EHR systems (Coats & Achyara, 2014, p. 2). This need for on-demand access has also increased through the use of mobile devices. Despite the amount of opportunities, cloud computing health information can be more vulnerable to privacy and security threats. More on the severity of these issues will be further discussed in the upcoming sections of this paper.

In today's fast paced society, physicians are favoring information technology (IT) systems that provide needed information quickly rather than securely. This is one of the many factors that has made health IT systems easier targets for hackers, as opposed to other industries, such as, retail and finance. Communicating health information electronically provides many benefits, but as more information is transferred via mobile devices, the range of targets in which hackers can access is increasing. According to the *2016 Data Breach Industry Forecast* from

Experian Data Breach Resolution, it is predicted that the amount of cyberattacks against hospitals and medical groups will continue to grow due to the value of the PII stored in medical records ("Hackers set," 2016). This prediction is significant to the future of healthcare organizations and the public's ability to trust how their health data is stored.

Privacy and Security Issues of Cloud Computing Health Information

One of the largest concerns with information stored in the cloud is the growing possibility of data theft. Over the past five years, data theft in the healthcare industry has more than doubled. According to a survey conducted by Ponemon Institute, nearly 90% of healthcare providers had experienced some sort of data breach within the past two years. Over half of those were the result of criminal activity ("THE CLOUD MOMENT," 2015). Hackers are beginning to set their sights on larger healthcare corporations because they are able to target massive amounts of PII, such as, birthdates, Social Security numbers, and credit card numbers, in one quick sweep. Steve Waldreen, MD, the director of the Alliance for eHealth Innovation at the American Academy of Family Physicians, states that, "Identity theft is a fruitful business, and there are some estimates that medical records are worth up to $50 each. But hackers are usually looking at larger institutions where they can potentially gain access to hundreds of thousands of files" (Waldreen, 2016).

When discussing privacy and security issues with cloud computing health information, it is important to understand HIPAA laws. In regards to the Health Insurance Portability and Accountability Act of 1996, HHS developed the HIPAA Privacy Rule and Security Rule. The Privacy Rule established national standards to protect certain health information. This rule requires healthcare organizations, referred to by HIPAA as "covered entities", to allow patient health records to be available for the purpose of medical treatments, either through a court order

or through signed patient consent. Patients must be notified of the use of their PHI by the organization. The Security Rule elaborates on the Privacy Rule by establishing national standards for protecting PHI created, maintained, and stored in electronic formats. Organizations must guarantee security of administrative, technical, and physical safeguards, while also ensuring the confidentiality, integrity, and availability of PHI (Rodrigues, 2013).

Types of Cloud Models. Just as not all cloud service providers offer the same support and services, not all cloud models are made the same. There are four main cloud types to choose from based on user needs, preferences, and desired privacy and security capabilities. When discussing privacy and security concerns, it is crucial to understand the differences between a public, private, hybrid, and community cloud models. Depending on the type of information to be stored in the cloud should dictate which model is chosen. Ensuring the security of PII should be the main concern of all organizations.

Public Cloud. Public clouds are owned by external vendors who provide users and organizations with the resources they need to have access to their stored information. Public clouds are shared computing environments, meaning multiple businesses, or users, share one cloud. Public cloud vendors are responsible for managing stored information and for maintaining the technology systems (Dinh, 2011, p. 36). This type of model is available online to anyone that has an internet connection. Users are typically residential users that connect to the internet through their internet service provider's network. The biggest concerns with the public cloud is the security and privacy of data. There is concern about where data is stored and whether or not unauthorized users have access. Some common examples of public cloud include Amazon, Google, and Microsoft Office 365 (Goyal, 2014, p. 23). This might be ideal for smaller businesses who cannot afford their own storage and IT personnel. Some organizations might also

choose this option because commercial vendors tend to invest more in enhancing usability features, such as, retrieving and resetting login information (Coats & Acharya, 2014). Each vendor's products provide different capabilities and features.

Private Cloud. For organizations needing to store larger amounts of information, a private cloud might be a better choice. This type is built within an organization's firewall, or can be space within a vendor's data center that is dedicated only to that organization. Private clouds are more costly because the organization must purchase and maintain the physical servers themselves. The benefits of this is that they know exactly where their stored data physically lives at all times, and there is more control over who has physical access to the data, which typically results in a more secure system. On the other hand, if the organization does not employ proper security measures, the data could be more at risk than in a public cloud.

Hybrid Cloud. The third type of cloud is the hybrid cloud, which uses a mixture of two or more cloud models, typically at least one public and one private. The public portion is managed by a third party vendor that stores less critical information that the organization might not otherwise have enough space to store. The private portion of the cloud is used for storing highly sensitive information in-house. This might seem like the best model offering the advantages of both a public and private cloud, but it also comes with their disadvantages as well. The hybrid cloud may require more security implementations.

Community Cloud. The community cloud is shared by multiple organizations that have the same concerns. Though this cloud model is still fairly new, it can be a more cost effective option by allowing organizations to share the costs associated with setting it up. The main drawback to this structure is the limited amount of bandwidth and data storage between all organizations involved (Goyal, 2014, p. 25).

Cloud Computing Security Mechanisms. Before employing a cloud based EHR management system, covered entities must focus on the administrative requirements. This includes designating the responsibilities of security to one or more individuals in the organization. The chief information security officer (CISO) should be in charge of all efforts of establishing and maintaining the protection of information, and the technology systems that store the information. A security management process must be developed to include policies and procedures for periodic risk analysis, risk management, sanction policy, and information system activity reviews. A proper contingency plan is also crucial. The contingency plan must outline the organization's data backup plan, disaster recovery, and emergency mode operations plan. Additionally, HIPAA's administrative requirements state that it is the information security department's responsibility to administer security training (Department of Health and Human Services, 2007).

When protecting PII store in the cloud, prevention is key. There are various security mechanisms that cloud vendors and healthcare organizations should incorporate into their systems. Physical safeguards focus on protecting the information systems and the equipment that stores the organization's data. The equipment must be protected from threats, environmental hazards, and unauthorized intrusions. Technical safeguards serve to protect data and control access to information stored in the EHR system and in the cloud. Safeguards should be used in conjunction with one another in order to ensure the best possible protection. For the purpose of this paper, technical safeguards will be the focus.

Password Protection. Requiring a password to access an account seems like an obvious thing to do. Most people assume that they will have to provide a password for just about any sort

of computer or internet login. It is important that health IT systems require more complicating passwords than the average account, therefore, making it more difficult for hackers.

At any given time, multiple different people may need to access a patient's record. This could be the patient themselves, nurses, physicians, IT personnel, etc. Access to PHI stored in the cloud should be limited to only what is needed for the person to adequately perform their job. Role based access controls are the most efficient way of controlling who is able to see certain parts of each record. Employees are issued an individually identifiable login name and password to log into the cloud. Not only does this limit who has access to what, but it also tracks which portions of the record are viewed, and includes a date and time stamp (Rodrigues, 2013).

Encryption of Data. Health information management professionals define data encryption as "the process of transforming text into an unintelligible string of characters that can be decrypted once it reaches a secure destination" (Butler, 2015). In other words, the PHI is transformed into a secret code that can only be translated the end user if they have the correct key or password. Data encryption is one of the best ways of preventing data breaches. It is crucial that any data stored in the cloud be encrypted.

Network Firewall. When working to protect PHI, healthcare professionals should be aware that the majority of threats will come from outside the organization, rather than from internal sources. Network security mechanisms is the next best way of preventing data breaches. Whenever an organization uploads medical records to the cloud, it exposes that information to several new threats by making it available on the internet. It is the responsibility of both the healthcare organization, and any third party cloud vendors or providers, to use strong network firewall protection (Rodrigues, 2013). Not only is it necessary to have a good firewall router, it is a good idea to go a step further in order to make the internal network seem as a black hole to

outsiders. Many professionals may not realize that they should change the password that was given when the router was installed. Wi-Fi should also be secured with a new password, and a change in the default name of the Service Set Identifier (SSID). The network router should be set so that it does not display the SSID (Terry, 2016, p. 82).

The adoption of cloud based EHR systems is continuing to grow, and industry trends show no signs of slowing down. With healthcare data theft on the rise, it is now, more than ever, crucial that security efforts are increased. The use of mobile devices for accessing health information stored in the cloud has made data more vulnerable to hackings. According to the Bitglass Healthcare Breach Report of 2016, there were reportedly10 million people affected by a data breach in 2015. Additionally, more than 111 million Americans had their health information lost due to hackers or other IT related incidents. Healthcare organizations seem to try and put the patients' minds at ease by emphasizing that their information is secure in an EHR, but with an 80% increase in data breach hacks from 2015 to 2016, it is hard to believe that current privacy and security efforts are effective (Pennic, 2016).

Despite governmental efforts to prevent and penalize negligent actions that can lead to the exposure of personal health information, a breach can result in permanent damages for its victims. Existing literature primarily focuses on the benefits of cloud computing, while briefly discussing the privacy and security issues that may arise. According to breach reports, the number of healthcare data breaches have steadily increased over the past five years. Further research is needed to investigate the probability of a relationship between the number of breaches and the widespread adoption of cloud computing. It is the purpose of this study to uncover the truths on the safety of storing PII and PHI in the cloud.

Chapter 3

Methodology

Research Design

A system review conducted through extensive research on existing literature relevant to the privacy and security issues of cloud computing PII and PHI. Database searches were performed using PubMed, CINAHL, and the American Health Information Management Association (AHIMA) Body of Knowledge. The following keywords were used : cloud computing, health information, security, and privacy. In order to provide a more comprehensive coverage of information, Google search engine was used to find additional information from reputable sources. Table 1 lists the keywords used in the search of each database, the search filters used, and the number of results provided. An evaluation of the search results was conducted by reading article titles and abstracts. The following inclusion and exclusion criterion were then applied.

Table 1

Keyword Search Strings by Database

Database	Search String(s) Used	Filters	Number of Search Results
PubMed	("cloud computing"[MeSH Terms] OR "cloud"[All Fields] AND ("privacy"[MeSH Terms] OR "privacy"[All Fields]) AND security[All Fields]) AND ("2011/10/28"[PDAT] : "2016/10/25"[PDAT]) AND ("2011/10/28"[PDat] : "2016/10/25"[PDat] AND English[lang])	Publication dates: past 5 years AND Language: English	84
CINAHL	"cloud computing" AND "security" AND "privacy"	Publication Dates: 2011 to 2016 Language: English Geography: USA	39
AHIMA Body of Knowledge	"privacy and security of cloud computing"	Publication Dates: 01/01/2011 to 10/01/2016	52
Google	"healthcare data breach statistics related to cloud computing"	Publication Dates: 01/01/2011 to 12/31/2016	Unknown

Inclusion Criteria

Eligible literature included peer-reviewed articles and information originating from reliable institutions. Only the articles that focused on privacy and security issues resulting from cloud computing PII and PHI, and healthcare data breaches were considered for evaluation.

Exclusion Criteria

Any literature that did not focus on the privacy and security of health information in the cloud was excluded from this study. Sources from outside of the United States were not included due to interoperability issues and the lack of international health information exchange standards.

Quality Assessment

After each article was assessed based on the inclusion and exclusion criterion previously listed, primary evaluation of titles and abstracts was conducted, the remaining articles were read

in full-text. Each article was analyzed to determine the quality of the information. Results from the quality assessment were used to determine inclusion in the study.

Data Collection

Data collected was used to determine the relationships between cloud computing and the privacy and security of PII and PHI. Data was obtained electronically using Google search and the databases previously mentioned. An initial assessment of each article was performed by reviewing the title and abstract to identify the presence of any inclusion or exclusion criterion as listed above, then assessed for quality. Relevant data was retrieved from the remaining articles, and combined and summarized to support the purpose of this study.

Chapter 4

Results

Search results from PubMed, CINAHL, and AHIMA Body of Knowledge yielded a total of 87 articles. An additional 12 were found through Google search, producing a combined total of 99 potentially relevant sources in the initial search. Through careful screening, 37 of the articles were chosen for further analysis. Full-text review and quality assessment narrowed the results down to 17 sources to be included in this study (see figure 1). Of these 17 sources, 4 studies and statistics reports were chosen to provide the quantitative data that led to the results of this study. Table 2 outlines the key characteristics and methodology of these studies. It is believed that each of the chosen sources provide complete insight into the privacy and security issues related to cloud computing health information, and answer the research questions stated in the introduction of this paper. The following sections will answer the research questions.

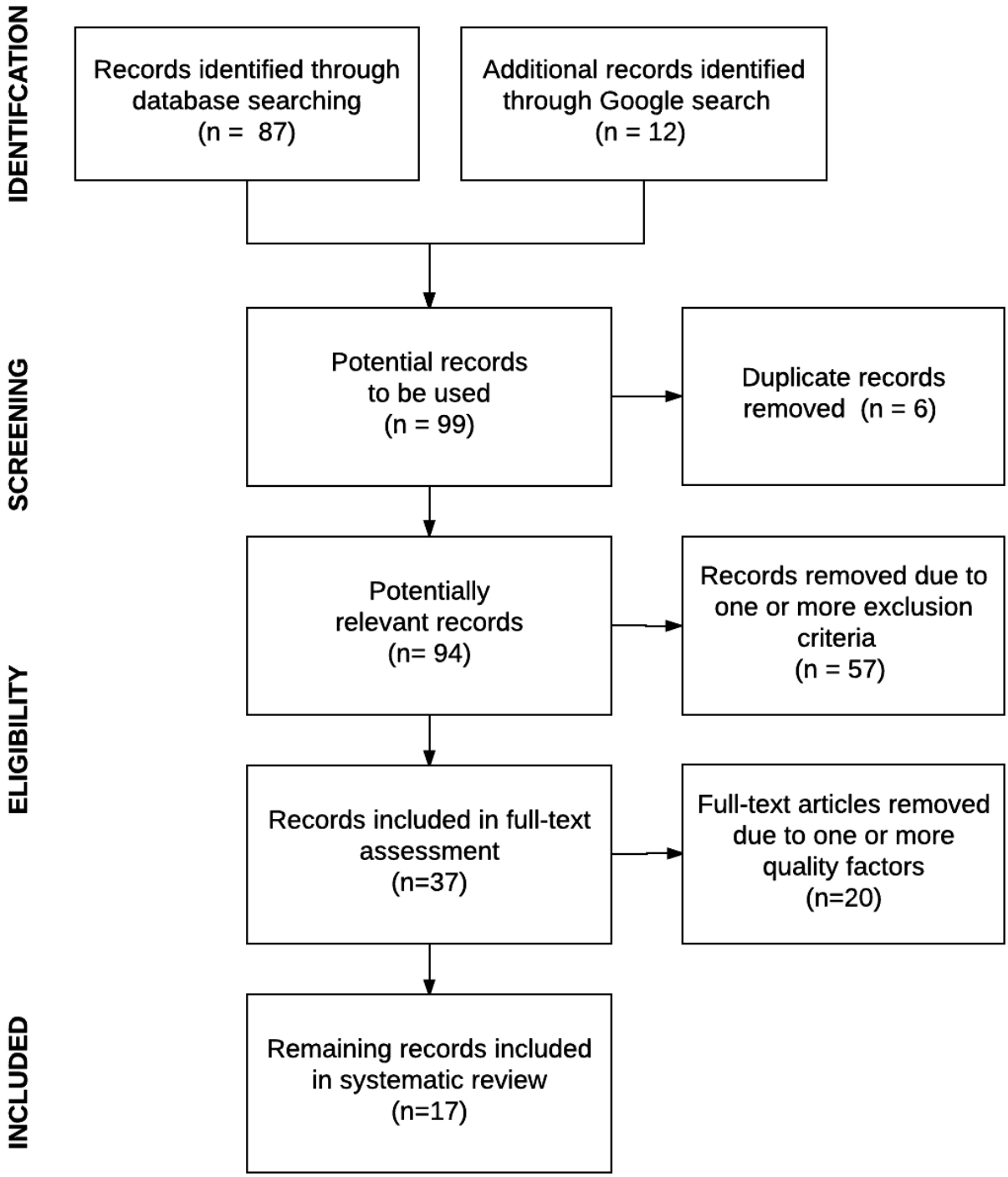
Table 2

Main Studies Focused on in Systematic Review

Study Title	Study Reference	Methodological Approach	Study Date(s)	Description of Study Population	Number of Respondents	Study Purpose
2014 HIMSS Analytics Cloud Survey	HIMSS Analytics	Web-based survey	March 26 through April 30, 201	IT Executives from Healthcare Provider Organizations	150; 3.4% response rate	Report usage of cloud based services and identify key areas of concern
Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data	Ponemon Institute	Survey	March 2016 to April 2016	IT Executives from Healthcare Provider Organizations	91 healthcare organizations and 84 business associates; 18% response rate	Identify the frequency of breaches and the prevention resources
Identity Theft Resource Center 2016 Data Breach Stats	Identity Theft Resource Center	Receives data from various media sources and/or notification lists from state and governmental agencies	January 1, 2016 to October 26, 2016	All healthcare organizations	n/a	Compilation of all data breaches that provides public access to up-to-date information.
ITRC Data Breach Statistics 2005 - 2015	Identity Theft Resource Center	Receives data from various media sources and/or notification lists from state and governmental agencies	January 1, 2005 to December 31, 2015	All healthcare organizations	n/a	Compilation of data breach statistics that provides public access to information

Figure 1

Flowchart of Data Reviewed

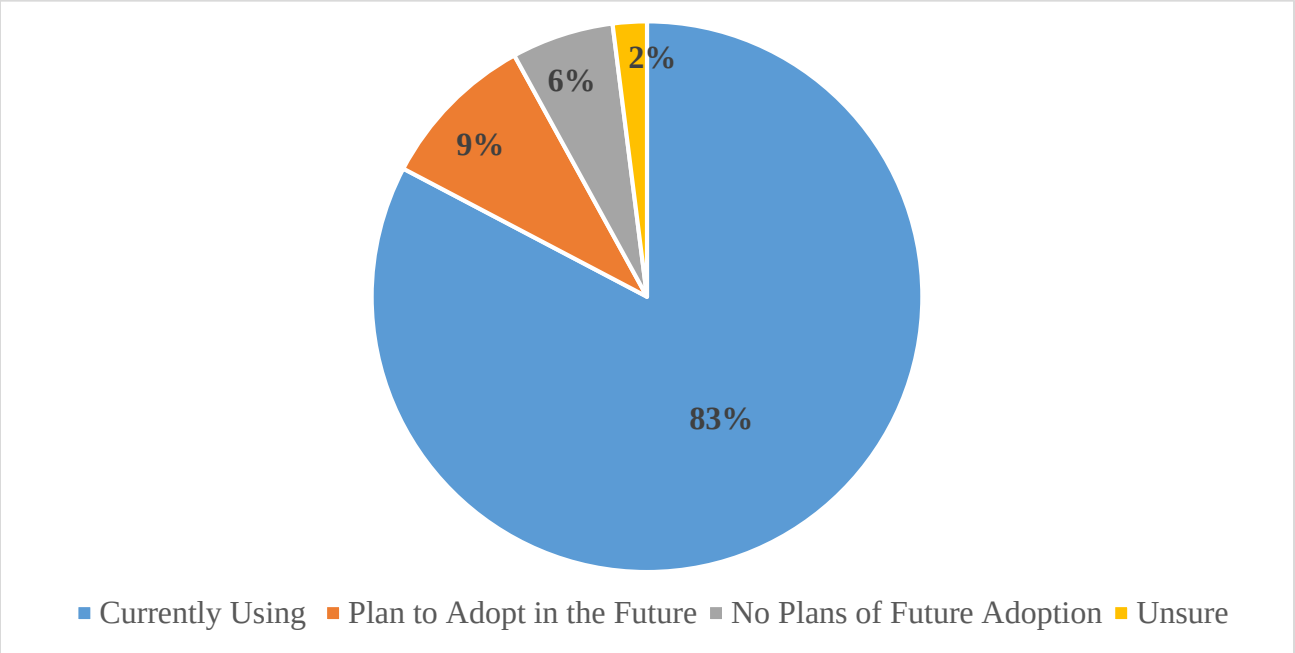


Cloud Computing Adoption Rates

In 2011 only 4% of healthcare organizations were using cloud computing. At that time it was estimated that the industry would experience a 20.5% increase in use between 2012 and 2017 (IBM Corporation, 2012, p. 2). According to the *2014 HIMSS Analytics Cloud Survey*, as of 2014, over 80% of organizations have adopted some form of cloud based technology (HIMSS Analytics, 2014, p. 8). Figure 2 shows the current usage rate in comparison to those who plan to adopt, do not plan to adopt, or are unsure of their future adoption plans. These numbers are based off the results of a survey given in 2014 to 150 large healthcare organizations by HIMSS Analytics. HIMSS Analytics is a professional organization that is well respected leader in providing valuable HIT market research.

Figure 2

Healthcare Organizations Cloud Computing Usage Rates in 2014



General Areas Where Cloud Based Services are being used

The respondents of the *2014 HIMSS Analytics Cloud Survey* labeled as "currently using" cloud based technology, were asked which general areas their organization was currently using cloud services. There were four areas to choose from: administrative functions, IT functions, clinical applications & data, and external data sharing. Each area contains the following uses:

Administrative Functions:

- Hosting of financial applications and data
- Hosting of operational applications and data
- Hosting of human resources (HR) applications and data
- Hosting of back office applications and data

IT Functions:

- Hosting of archived data
- Backups and disaster recovery
- Hosting of communications services (for example, e-mail, voice communications, etc.)
- Identity management
- Timely provisioning and deprovisioning of user accounts
- Desktop virtualization
- Server virtualization
- Virtual networks
- Managed service

Clinical Applications & Data:

- Hosting of clinical applications and data

External Data Sharing:

- Health Information Exchange
- Accountable Care Organizations

As shown in table 3, administrative and IT functions were ranked as the largest areas with 73.4% usage rates over the other areas tested. Most respondents reported using cloud based services for hosting of financial, operational, or HR data. IT functions were most commonly reported as traditional functions such as hosting archived data and virtualization (HIMSS, 2014, p. 10).

Table 3

General Areas Where Organizations Reported Using Cloud Based Services

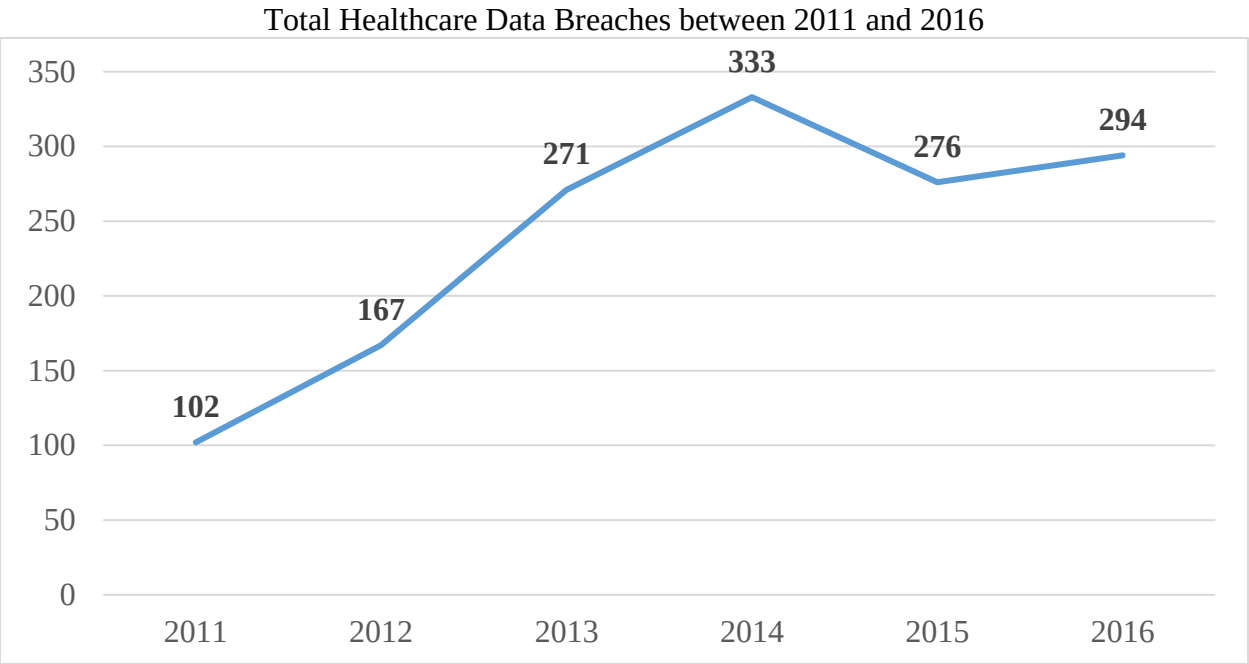
Area	Frequency	Total
Administrative Functions	91	73.4%
IT Functions	91	73.4%
Clinical Applications & Data	65	52.4%
External Data Sharing	60	48.4%
Total	124	100%

SOURCE: *2014 HIMSS Analytics Cloud Survey*

Healthcare Data Breach Statistics

Mirroring the increase in cloud computing usage is the amount of healthcare data breaches. In 2011 there were a reported 102 data breaches in the healthcare industry alone. Figure 3 illustrates a rapid increase in total number of breaches reported for the years 2011 to 2016. As shown, healthcare data breaches hit an all-time high in 2014 with a total of 333 breaches, which was calculated to equal 42.5% of all breaches across five industries. This followed by a slight decrease in 2015, but according to up-to-date reports from the Identity Theft Resource Center, 2016 has already shown a return in the growth trend (Identify Theft Resource Center, 2016, p. 1).

Figure 3



NOTES: Amount shown for 2016 is the total number of breaches reported as of October 25, 2016.

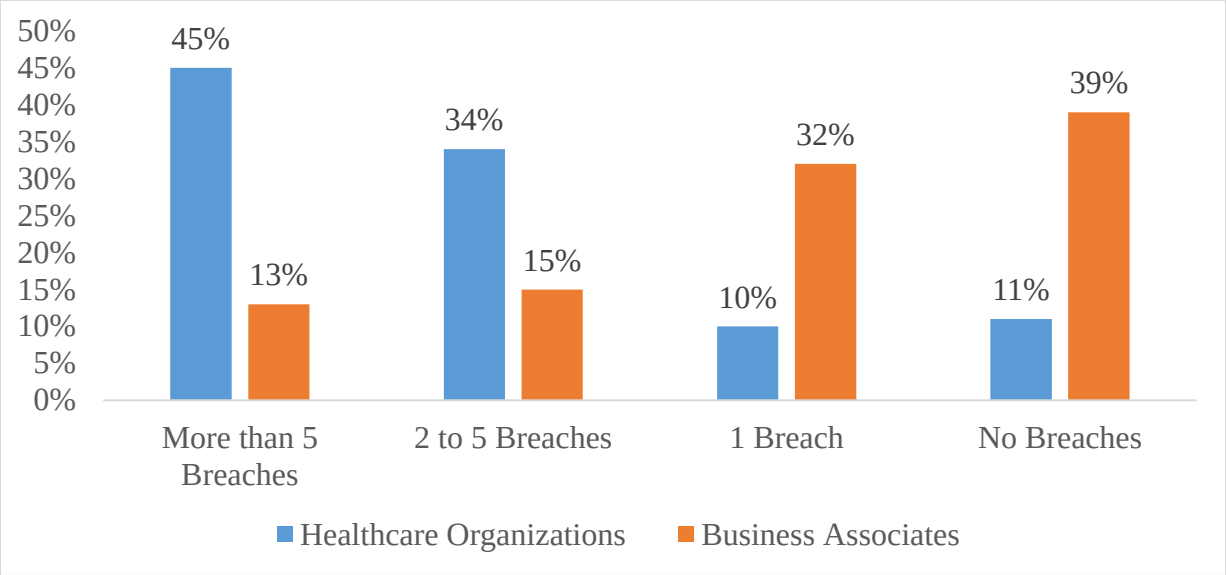
As of May 2016, according to *The Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data,* it is estimated that healthcare data breaches are costing the industry $6.2 billion dollars. 89% of healthcare organizations have reported having at least one breach that resulted in the theft or loss of patients' PII or PHI. Figure 4 shows a comparison of the amount of breaches experienced by covered entities and healthcare business associates within the past 24 months. 61% of business associates reported having at least one data breach in the past 24 months, with 28% reporting more than two (Ponemon Institute, 2016, p. 19).

The records that contain the most sensitive patient data includes medical files and billing and insurance information. The information in these files are highly targeted by criminals because the resale value on the black market is estimated to be up to $363 per record. Figure 5 shows that healthcare organizations have experienced an increase in the loss or theft of sensitive

patient data between 2015 and 2016. As shown, there was a 9% increase in the theft of medical files alone. Medical files are now more sought after by criminals than are credit card numbers (Ponemon Institute, 2016, p. 21).

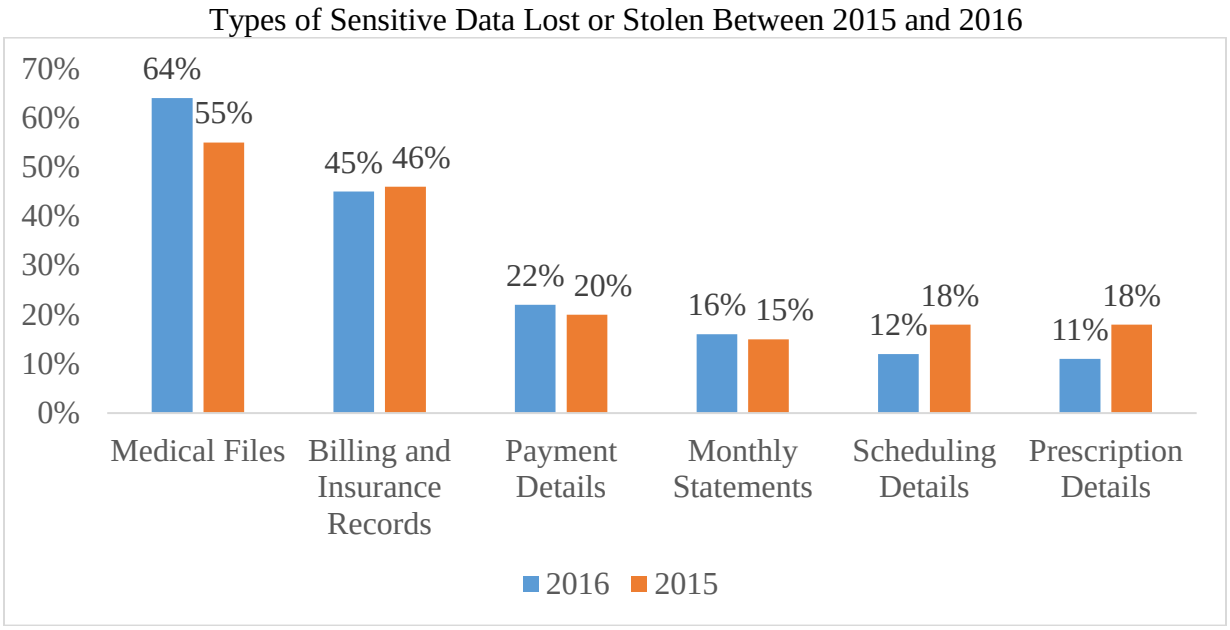
Figure 4

Healthcare Data Breaches Experienced by Healthcare Organizations and Business Associates



NOTES: Percentages are based on breaches involving loss or theft of patient data within the past 24 months of when the study was published in May 2016.
SOURCE: *The Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data*

Figure 5



SOURCE: *The Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data*

Chapter 5

Analysis and Discussion

As outlined in the above results section, there is an obvious increase in the adoption of cloud based services in the healthcare industry. Industrywide adoption rate went from 4% in 2011 to 83% in 2014 as reported by HIMSS Analytics (HIMSS Analytics, 2014, p. 8). With a significant increase such as this, it is important to research and analyze the possible outcomes on the sensitive data that these systems manage. As shown in table 5, there are 4 general areas that respondents to the *2014 HIMSS Analytics Cloud Survey* were asked to indicate their organization's usage of cloud based services. Administrative and IT functions were ranked as the most used areas specifically for hosting financial data, operational data, HR data, and archived data. This means that 73.4% of organizations are using cloud services for storing or managing the most sensitive types of patient data, PII and PHI.

The first research question of this study is how much have healthcare data breaches increased since cloud computing became more widely used? From the review of research, it was found that the use of cloud computing began rapidly increasing after 2011 when the industry shifted its focus towards improving HIT. Looking at the amount of data breaches from 2011 to 2016 shows a rapid increase over the past five years. Therefore, from the 102 breaches in 2011 to the 294 in 2016, it is calculated that there has been a 188% increase in the amount of healthcare data breaches since cloud computing became more widely used in healthcare.

The second research question aims to answer whether or not the increase in data breaches and the use of cloud based services are directly related. According to IBM, five of the eight largest data breaches that the industry has seen in the past five years occurred in the first few months of 2015. Over 100 million medical records were exposed, but surprisingly only one

breach was reported as being directly related to cloud based service. Out of the other breaches reported, none had any business associates involved, such as third party cloud vendors. It was found that out of 242 breach incidents, 46% were caused by portable devices such as laptops, hand-held devices (cell phones and tablets), paper, or film (Van Deursen, 2015). From these results, it can be concluded that increased used of cloud computing does not cause data breaches. Additional research is needed to determine the root causes of breaches in order to help organizations avoid them in the future. The one cloud related security breach from 2015 has not divulged any insight as to how it occurred.

The third and last research question asks the definitive question that all current and potential users of cloud based services want to know; is PII and PHI stored and managed in the cloud secure? With few reports of cloud related data breaches in healthcare, it appears as if organizations and cloud vendors' current security efforts are effective. While information in the cloud might be secure, for now, it poses a higher risk for a larger and more costly outcome should a breach occur. Ponemon Institute's *Data Breach: The Cloud Multiplier Effect,* found that as the amount of records breached reaches over 100,000, the costs can increase from the average 2.73 million to 5.32 million (Ponemon Institute, 2014, p. 1). This study finds that information is in fact secure in the cloud, but organizations and cloud vendors need to continue being proactive to ensure that cloud based breaches remain low.

Limitations

- Review of the literature reveals that little research exists on the security of cloud computing health information. Additional research is needed.
- The research that is available only represents a small portion of the healthcare organizations using cloud based services.

- There are not enough studies that accurately portray the current market conditions for cloud computing and data privacy and security.

Chapter 6

Conclusion

The adoption of cloud based EHR systems is continuing to grow, and industry trends show no signs of slowing down. With healthcare data theft on the rise, it is now, more than ever, crucial that security efforts are increased. The use of mobile devices for accessing health information stored in the cloud has made data more vulnerable to hackings. According to the Bitglass Healthcare Breach Report of 2016, there were reportedly10 million people affected by a data breach in 2015. Additionally, more than 111 million Americans had their health information lost due to hackers or other IT related incidents. Healthcare organizations seem to try and put the patients' minds at ease by emphasizing that their electronically stored health information is safe, but with an 80% increase in data breach hacks from 2015 to 2016, it is hard to believe that current privacy and security efforts are effective (Pennic, 2016).

Organizations that experience a data breach may be subject to civil or criminal penalties. Despite the government's efforts to penalize users' negligent actions, a data breach can have irreversible effects on its victims. The true victims in these crimes are the patients who have to suffer the consequences of having their most confidential information in the hands of criminals. Cloud computing health information brings many opportunities to healthcare, but unfortunately, there are many issues that still remain.

The purpose of this study was to determine how healthcare data breaches have increased or decreased since the use of cloud based services began increasing in 2011, whether or not the change in data breach statistics is a direct result of increased cloud adoption, and if PII and PHI

is safe in the cloud. Through extensive research and systematic review, it was determined that data breaches have significantly increased since 2011. Industry experts predict that privacy and security threats will continue to grow in the upcoming years. At this time, it does not appear that cloud computing is directly related to the occurrence of recent breaches, but additional studies are desperately needed to further determine a definitive answer. The healthcare industry would greatly benefit from further research on this topic.

References

Butler, M. (2015). Cracking Encryption: Despite Benefits, Technology Still Not Widely Used to Combat Multi-Million Dollar Breaches. *Journal of AHIMA*. Retrieved from http://bok.ahima.org/doc?oid=107594#.V4av4o-cFjo

Coats, B., & Acharya, S. (2014). Leveraging the Cloud for Electronic Health Record Access. *Perspectives in Health Information Management*, 1-19. Retrieved from http://bok.ahima.org/doc?oid=301201#.V4UOk4-cHIU

Department of Health and Human Services. (2007). *HIPAA Security Series: Security 101 for Covered Entities*. Retrieved from Department of Health and Human Services website: http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/security101.pdf

Dinh, A. K. (2011). Cloud Computing 101. *Journal Of AHIMA, 82*(4), 36-37. Retrieved from http://bok.ahima.org/doc?oid=103806#.V4T7Q4-cHIV

Goyal, S. (2014). Public vs private vs hybrid vs community - cloud computing: A critical review. International Journal of Computer Network and Information Security, 6(3), 20-29. doi:10.5815/ijcnis.2014.03.03

Hackers setting their sights on healthcare. (2016). *Doctor's Office, 35*(6), 1-5.

Healthcare cloud barriers still exist. (2015). *Healthcare Leadership Review, 34*(2), 12-13.

HIMSS Analytics. (2014). *2014 HIMSS Analytics Cloud Survey*. Retrieved from Healthcare Information and Management Systems Society website: http://s3.amazonaws.com/rdcms-himss/files/production/public/FileDownloads/Final%20Report%20061214.pdf

IBM Corporation. (2012). *For healthcare, change is in the air—and in the cloud* (GMW14023-

USEN-00). Retrieved from https://www-05.ibm.com/de/healthcare/pdf/For_healthcare_change_is_in_the_air_-_and_in_the_cloud.pdf

Identity Theft Resource Center. (2016). *ITRC Breach Statistics 2005 - 2015*. Retrieved from http://www.idtheftcenter.org/images/breach/2005to2015_20160828.pdf

McCallister, Erika. (2010). *Guide to protecting the confidentiality of Personally Identifiable Information (PII): Recommendations of the National Institute of Standards and Technology*. Retrieved from U.S. Dept. of Commerce, National Institute of Standards and Technology website: http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

Pennic, F. (2016, January 28). Report: Hackers Caused 98% of Healthcare Data Breaches. Retrieved from http://hitconsultant.net/2016/01/28/hackers-caused-98-of-healthcare-data-breaches/

Ponemon Institute. (2014). *Data Breach: The Cloud Multiplier Effect*. Retrieved from http://go.netskope.com/rs/netskope/images/Ponemon-DataBreach-CloudMultiplierEffect-June2014.pdf

Ponemon. (2016). *Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data*. Retrieved from http://lpa.idexpertscorp.com/acton/attachment/6200/f-04aa/1/-/-/-/-/Resources%20-%20Sixth%20Annual%20Benchmark%20Study%20on%20Privacy%20and%20Security%20of%20Healthcare%20Data%20.pdf?cm_mmc=Act-On%20Software-_-email-_-ID%20Experts%20Download%20-%20Sixth%20Annual%20Benchmark%20Study%20on%20Privacy%20%26%20Security%20of%20Healthcare%20Data-_-Download%20Now&sid=TV2:yfvRfTa6Q

Rodrigues, J. J. (2013). Analysis of the Security and Privacy Requirements of Cloud-Based Electronic Health Records Systems. *Journal of Medical Internet Research*, *15*(8). Retrieved from http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3757992/

TERRY, M. (2016). How Is Your Computer Security?. *Podiatry Management*, *35*(4), 79-86.

THE CLOUD MOMENT IN MEDICINE. (2015). *Healthcare Informatics*, *32*(6), 24-27.

U.S. Department of Health & Human Services. (2016). HIPAA for Professionals | HHS.gov. Retrieved from https://www.hhs.gov/hipaa/for-professionals/index.html

U.S. Department of Health and Human Services National Institutes of Health. (2007, February 2). What Health Information Is Protected by the Privacy Rule? Retrieved from https://privacyruleandresearch.nih.gov/pr_07.asp

Van Deursen, N. (2015, December 18). 2015 Was the Year of the Health Care Data Breach, but Cloud Sails Around the Storm. Retrieved from https://securityintelligence.com/2015-was-the-year-of-the-health-care-data-breach-but-cloud-sails-around-the-storm/

Waldreen, S. (2016). Hackers setting their sights on healthcare. *Doctor's Office*, *35*(6), 1-5.