


4-2016

# Using security risk analysis: Is the bring your own device policy becoming a liability risk within healthcare?

Lee Alexander Cavett  
*Purdue University*

Follow this and additional works at: [https://docs.lib.purdue.edu/open\\_access\\_theses](https://docs.lib.purdue.edu/open_access_theses)

 Part of the [Health and Medical Administration Commons](#), and the [Health Information Technology Commons](#)

---

## Recommended Citation

Cavett, Lee Alexander, "Using security risk analysis: Is the bring your own device policy becoming a liability risk within healthcare?" (2016). *Open Access Theses*. 757.  
[https://docs.lib.purdue.edu/open\\_access\\_theses/757](https://docs.lib.purdue.edu/open_access_theses/757)

This document has been made available through Purdue e-Pubs, a service of the Purdue University Libraries. Please contact [epubs@purdue.edu](mailto:epubs@purdue.edu) for additional information.

**PURDUE UNIVERSITY  
GRADUATE SCHOOL  
Thesis/Dissertation Acceptance**

This is to certify that the thesis/dissertation prepared

By Lee Alexander Cavett

Entitled

USING SECURITY RISK ANALYSIS: IS THE BRING YOUR OWN DEVICE POLICY BECOMING A LIABILITY RISK WITHIN HEALTHCARE?

For the degree of Master of Science

Is approved by the final examining committee:

Dr. James Eric Detiz

Chair

Dr. Eric Matson

Dr. Pamela Aaltonen

To the best of my knowledge and as understood by the student in the Thesis/Dissertation Agreement, Publication Delay, and Certification Disclaimer (Graduate School Form 32), this thesis/dissertation adheres to the provisions of Purdue University's "Policy of Integrity in Research" and the use of copyright material.

Approved by Major Professor(s): Dr. James Eric Dietz

Approved by: Jeffrey Whitten

Head of the Departmental Graduate Program

4/22/2016

Date



USING SECURITY RISK ANALYSIS: IS THE BRING YOUR OWN DEVICE  
POLICY BECOMING A LIABILITY RISK WITHIN HEALTHCARE?

A Thesis

Submitted to the Faculty

of

Purdue University

by

Lee A. Cavett

In Partial Fulfillment of the

Requirements for the Degree

of

Master of Science

May 2016

Purdue University

West Lafayette, Indiana

## ACKNOWLEDGMENTS

I wish to acknowledge my committee members: Dr. James Eric Dietz, Dr. Pamela Aaltonen, and Dr. Eric Matson. Thank you for all the valuable and encouraging insight and guidance throughout my research experience. I would also like to acknowledge my roommates. They motivated me to stay focused and to always remember what is at stake - thanks GiJey Gilliam, Mark Pengatore, and Jarrod Crutcher. Most importantly, I would like to thank my family.

## TABLE OF CONTENTS

	Page
LIST OF TABLES . . . . .	v
LIST OF FIGURES . . . . .	vi
ABBREVIATIONS . . . . .	vii
ABSTRACT . . . . .	viii
CHAPTER 1. INTRODUCTION . . . . .	1
1.1 Scope . . . . .	1
1.2 Research Question . . . . .	2
1.3 Significance . . . . .	2
1.4 Assumptions . . . . .	3
1.5 Limitations . . . . .	3
1.6 Delimitation . . . . .	3
1.7 Definitions . . . . .	4
1.8 Summary . . . . .	5
CHAPTER 2. REVIEW OF RELEVANT LITERATURE . . . . .	6
2.1 Security Risk Leading into Data Breaches . . . . .	6
2.1.1 BYOD Policy . . . . .	10
2.1.1.1 iPads . . . . .	11
2.2 Budget . . . . .	13
2.3 Government Guidelines . . . . .	15
2.4 Breach Notification . . . . .	17
2.5 Summary . . . . .	18
CHAPTER 3. METHODOLOGY . . . . .	20
3.1 Theoretical Framework . . . . .	20
3.1.1 AnyLogic . . . . .	20
3.2 Sample Set . . . . .	21
3.3 Testing Methodology . . . . .	21
3.4 Chapter Summary . . . . .	23
CHAPTER 4. PRESENTATION OF DATA . . . . .	24
4.1 Initial Inputs and Parameters . . . . .	24
4.2 Process . . . . .	25
4.3 Recorded Data Collection . . . . .	25
4.4 Calculated Risk . . . . .	26

	Page
CHAPTER 5. CONCLUSION . . . . .	29
APPENDIX A. HEALTH CLINIC LAYOUT . . . . .	31
APPENDIX B. BYOD SIMULATION MODEL . . . . .	32
APPENDIX C. DESKTOP SIMULATION MODEL . . . . .	33
APPENDIX D. DEMONSTRATE MATHEMATICS . . . . .	34
LIST OF REFERENCES . . . . .	35

## LIST OF TABLES

Table	Page
2.1 Parameters and Tier Violations . . . . .	19
4.1 Model Parameters . . . . .	25
4.2 Model Results: Wireless vs. Wired . . . . .	26
4.3 Model Run 1: Wireless Device . . . . .	26
4.4 Model Run 2: Wired Device . . . . .	26
4.5 Risk Value Input . . . . .	27
4.6 Risk Solutions . . . . .	27



## LIST OF FIGURES

Figure	Page
2.1 Reasons Medical Identity Theft Incident Not Reported (Ponemon Institute, 2015) . . . . .	8
2.2 Android vs. Apple Ownership Comparison (ClickCare, 2014) . . . . .	11
2.3 U.S Healthcare Total Government Spending (Five-Year Period) (Chantrill, 2015) . . . . .	15
3.1 Simulation Flow Diagram . . . . .	22
A.1 Health Clinic Layout . . . . .	31
B.1 BYOD Simulation Model . . . . .	32
C.1 Desktop Simulation Flow . . . . .	33

## ABBREVIATIONS

BYOD	Bring Your Own Device
EHR	Electronic Health Record
EMR	Electronic Medical Record
HHS	Department of Human and Health Science
HIPAA	Health Insurance Portability and Accountability Act
HITECT	Health Information Technology for Economic and Clinical Health
SBNL	Security Breach Notification Laws

## ABSTRACT

Cavett, Lee A. M.S., Purdue University, May 2016. Using Security Risk Analysis: Is The Bring Your Own Device Policy Becoming A Liability Risk Within Healthcare?. Major Professor: James E. Dietz.

Using computer simulation modeling, this research examined the problems contributing to data breaches within the healthcare industry. The study attempted to answer two questions: 1) is the Bring Your Own Device policy becoming a liability risk within health clinics causing an increase in data breaches and 2) is there a lower risk using Bring Your Own Device within the clinic compared to using desktop computers. iPad was the primary focused device as one of many Bring Your Own Devices. The study used a randomly generated sample of an approximate 2,700 patients, one nurse and doctor on a eight hour work-day within the clinic (eight A.M - five P.M) considering a one hour lunch break in between. The outcome of the study revealed that the Bring Your Own Policy had a lower risk than using desktops within health clinics.

## CHAPTER 1. INTRODUCTION

Over the last decade, healthcare organizations have increasingly embraced automation of medical information including the usage of Electronic Health Records (EHR). As the amount of electronic data being handled by healthcare systems continue to increase, it has become more of a focal point of emerging threats and vulnerabilities. Patients' secure data are often comprised due to data breaches. Security rules had been more recently promulgated but critics point to data breaches that result from a lack of proper protection on healthcare systems and equipment containing sensitive data. Many health organizations implemented a Bring Your Own Device (BYOD) policy which allow employees to use their device for medical usage. BYOD is commonly being use throughout many hospitals which could possibly be the cause of an increase in data breaches. The researcher analyzed if the BYOD policy is consider a liability risk by comparing wireless devices to desktop computers.

### 1.1 Scope

In this study, the researcher analyzed and determined if the BYOD policy was becoming a liability resulting to an increase data breaches as it continued to rise within healthcare. To narrow the number of smart hand-held devices used by many personal users; the particular device that was focused on was Apple Inc.'s iPad 9.2 iOS version. To reduce the complexity of the project, it was proposed that the researcher focus on the issues that are leading into data breaches within the healthcare clinic.

## 1.2 Research Question

- Based on increasing threats to IT infrastructure, are iPads becoming a liability risk within healthcare clinics?
- Comparing iPads (as one of many wireless BYODs) to desktop computers, which has the lowest risk factor within a healthcare clinic?

## 1.3 Significance

The U.S government allocated approximately 19 billion a year in funding for programs to help healthcare providers implement EHR as part of the economic stimulus package enacted in February 2009 (Bardhan & Thouin, 2012). Usage of EHR necessitates a more critical look at data security. The use of EHR increased throughout many hospitals and clinics, which was also leading into an increase of revenue. Proposals suggested that integrated EHR provided several benefits, some of which included: a reduction in costs, improved quality of care, the promotion of evidence-based medicine, enhanced record keeping and mobility (Fernandez-Aleman, Senor, Lozoya, & Toval, 2013).

However, with EHRs being interconnected, there had been several data breach reports which has emerged over the years; let alone, a BYOD policy can be used for doctors to access patient records while working. Few IT leaders saw iPads as healthcare “game-changers,” especially with the view of iPad EHR implementations as a way to promote useful compliance for physicians (ClickCare, 2014). Therefore, defining if the BYOD policy is causing an increase of data breaches is imperative. This determination could also aid hospitals to increase patients’ trust and help patients feel safe and secure with healthcare institutions holding their critical information.

#### 1.4 Assumptions

The assumptions for this study included:

- iPads (iOS 9.2 version) are most commonly used by staff within clinics.
- Franciscan St. Elizabeth Health - Lafayette East Health was the closest health facility in Lafayette, IN utilizing current health IT systems.

#### 1.5 Limitations

The limitations for this study included:

- iPads is the primary device as one of the several Bring Your Own Devices used within the health clinic.
- One business day (eight A.M to five P.M) was the time frame within the simulation model to conduct the research.
- The study focused on the the risk, negligence, and time when the staff in the treatment room with the patient.
- HIPAA's tier one violation was possible cause of a data breach throughout the model.

#### 1.6 Delimitation

The delimitation for this study included:

- The researcher did not focus on the risk factors outside of the health clinic.
- The researcher did not focus on all mobile devices and tablets used within the hospital.
- The researcher did not focused on risk of patient in the rest area or outside clinic.

## 1.7 Definitions

In the broader context of thesis writing, the author defines the following terms:

*Breach:* unauthorized acquisition, access, use, or disclosure of protected health information (HealthIT.gov, 2009).

*Electronic Health Records:* is used primarily for purposes of setting objectives and planning patient care, documenting the delivery of care and assessing the outcomes of care. It includes information regarding patient needs during episodes of care provided by different health care professionals (Hayrinen, Saranto, & Nykanen, 2008).

*Electronic Medical Records:* a digital version of a paper chart that contains all of a patients medical history. It is mostly used by providers for diagnosis and treatment (Fowler, 2015).

*Health Information Technology for Economic and Clinical Health:* is a law that was passed in 2009, designed primarily to modernize the flow of health information (Solove, 2013).

*Health Insurance Portability and Accountability Act:* is a law passed by Congress in 1996 [and amended over time] to regulate and protect the confidentiality of personal health data collected and used by health care organizations (Fowler, 2015).

*Security Breach Notification Laws:* are laws should provide American businesses with incentives to make significant changes in the way they handle and store consumer information in order to reduce the risk of data breaches (Winn, 2009).

*Social Engineer:* “is a technique an outside hackers use of psychological tricks on legitimate users of a computer system, in order to obtain information he needs

to gain access to the system, or getting needed information (for example, a password) from person rather than breaking into a system” (Granger, 2001).

### 1.8 Summary

This chapter provided the scope, significance, research questions, assumptions, limitations, delimitation, definitions, and other background information for the research project. The next chapter provides a review of the literature relevant of Electronic Health Records.



## CHAPTER 2. REVIEW OF RELEVANT LITERATURE

Technology has made a huge impact in the healthcare industry including record keeping. Earlier, medical records was stored in a paper format in large patient record storage closets. Filing and writing patients critical information by hand seems time consuming compared to the high-end technology used today. Medical records includes a great deal of sensitive information such as: personal information (driver license number, social security number, and date of birth insurance); medical diagnoses; treatment interventions; and financial information. Patients believe that this sensitive information will be shared appropriately and safeguarded. Policymakers push initiatives to bring healthcare into the digital age (Nigrin, 2014). With the increase of technology, healthcare workers have or are moving paper patient record keeping to electronic record keeping. In the healthcare industry, this is better known as Electronic Medical Record (EMR) or Electronic Health Record (EHR). With hospitals transitioning from filing patients' records in storage cabinets to electronically storing records, it's imperative to address security risk factors that could potentially lead a breach.

### 2.1 Security Risk Leading into Data Breaches

As in any other industry, in addition to safeguarding against the compromise of sensitive data, healthcare entities must now protect themselves against direct attacks meant to disrupt operations (Perakslis, 2014). Personal health records and other services that enable consumers to store and manage their own or their families' health information are now being control by third parties such as: Google and WebMD; these are also considered risk factors for data breaches (McGraw, Dempsey, Harris, & Goldman, 2009). According to the Health Insurance Portability

and Accountability Act (HIPAA), consumers have the right to access their medical records including the right to receive a copy “in the form or format requested,” if those records are “readily producible” in that format (McGraw et al., 2009). Often times, information such as personal data or identification is shared by the consumer.

When personal data is shared, it is a major risk and can possibly result in identity fraud. Ponemon (2013), a research center focused on data protection and information security policy, conducted a survey of 807 consumers who had self-reported medical identity theft. Thirty-one (31) percent had voluntarily shared identity credentials with a family member. When asked why, 92 percent did so because their family member lacked health insurance, 89 percent because the individual could not afford to pay for medical treatments, and 67 percent did so in a healthcare emergency. Medical identities use for trading could result in accounting and financial information that can be used to sell to third parties for malicious intent. In fact, EHR have 50 times the black market value of a credit card (Bitglass, 2014). In these types of situations, victims could possibly experience identity fraud, theft, or other possible attacks involving his or her medical record; however, the victim will not report the incident as shown in Figure 2.1 (Ponemon Institute, 2015).

Employees do their best to ensure patients’ EHR information is safe and secure; however, the value of EHRs were probed according to research. Recent studies have questioned the value of EHRs and clinical decision support systems and their impact on the quality of patient care; however, policymakers may find it necessary to go further and prohibit certain uses or disclosures of data in Personal Health Records, regardless of consent (Bardhan & Thouin, 2012; McGraw et al., 2009). Personal health data also are migrating onto the Internet through an exploding array of health information sites, support groups, and other on-line health tools, which falls outside of HIPAA unless they are being offered by covered entities (McGraw et al., 2009).

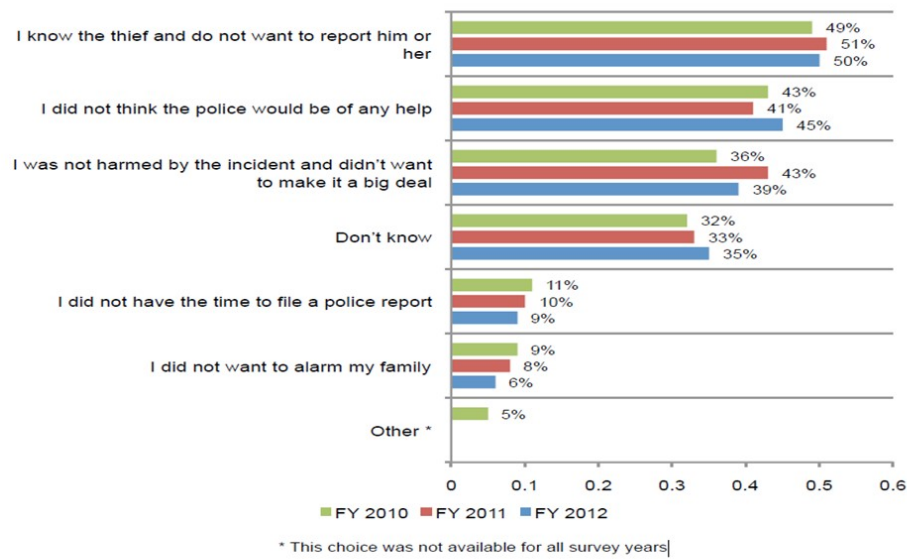


Figure 2.1. Reasons Medical Identity Theft Incident Not Reported (Ponemon Institute, 2015)

Besides gaining access to hospital information systems, computer viruses and malware can infect clinical monitoring devices; more so, network devices used by medical personnel such as smart devices used by doctors and nurses, even surgically implanted electronic devices (Kierkegaard, 2011). Having a virus infecting clinical monitoring devices or networked devices can be a scary situation especially if the staff is in the process of examining a patient. As compared to traditional IT systems involving incidents, such as a hacked MRI machine, can carry physical consequences as well as policy and financial impacts (Filkins, 2015). Anything that is interconnected could be in risk of being hacked. It could be argued often times EHR system that is purchased from outside vendors comes with pre-set privacy and security capabilities (Fernandez-Aleman et al., 2013). Purchasing through outside vendors is also known as outsourcing.

Outsourcing aids health organizations in many ways. Outsourcing reduces operational and software cost which results in a main critical advantage; however, outsourcing has its disadvantages. Significant outsourcing occurs in order to store patients' medical information. For instance, some of the EHR software packages includes: MediTouch, WRS Health, Modernizing Medicine, etc.) According to Wright (2004), sharing software with an outsourcing firm could cause a breach in the organization's licensing agreement or a copyright infringement. The level of accessibility rises when there are several third parties involve. The usage of a third party (using outside sourcing) allowing joint access of the EHR software could result into various users having access to the providing health organizations system. This development increases the chances of the system being breach. Despite outsourcing commonly used within businesses, the vulnerabilities involved are crucially demanding. With the numerous of outsourcing firms involved, it put data such as: credit card information, EHR, and account information at risk. As a result, when third parties are included, the organization may lose control over its system security administration creating a huge effect against the organization, according to Wright (2004)'s study.

Ponemon Institute (2015) mentions that employee negligence (70 percent) is the main security risk followed by use of public cloud services and cyber attackers (Ponemon Institute, 2015). A technique that is used but without significant on is social engineering. This attack can occur without the employees' awareness. When this technique is being applied, plenty of information can be retrieved and mostly occurs as manipulation through a psychological approach. "A social engineering tactic can be used by an attacker to gain illegal access to the pseudonymisation algorithm or the patient list, thus compromising the system," explained by Fernandez-Aleman et al. (2013). This technique can occur in several ways. Social engineering methods includes: phone, dumpster diving, on-line, persuasion, and reverse social engineering using public information. Each method results to either password and/or username comprise to an employee or EHR files (Granger, 2001).

Healthcare industries and many other companies have tons of trash that are being disposed at the end of the day; in healthcare, maybe the most simple method for an intruder. According to Granger (2001), types of material that could be used for possible data breach found in the dumpster are: organizational charts, memos, company phone books, company policy manuals, calendars of meetings, system manuals, printouts of sensitive data or login names and passwords, printouts of source code, and outdated hardware (Granger, 2001). Another security risk that may not seem as a threat now, but could possibly become a major security risk in the future is the BYOD policy.

### 2.1.1 BYOD Policy

The BYOD policy was initiated in the year 2009 by a top IT company and it pertains to the policy of allowing employees to bring privately owned devices such as smartphones, tablets and laptops into their workplace for usage and access to company applications and information (ClickCare, 2014). Healthcare providers typical that the Health Information Technology Department ensures that data and network on mobile devices is safe and secure in larger organizations. With BYOD becoming commonly used within the healthcare industry, it could also present a security concern. Eighty-eight (88) percent of organizations permit employees and medical staff to use their own mobile devices to connect to their organizations networks or enterprise systems (Ponemon Institute, 2015). BYOD allows health organizations the opportunity to increase efficiency and flexibility using EHR systems; however, the level of accessibility increases the system vulnerability and potential for data loss from BYOD lost devices.

To go in-depth of BYOD, there are several smart devices that can be use in hospitals. iPad represents a significant portion of mobile devices employed in healthcare; in addition will most likely to benefit from 4G technology in the coming years (ClickCare, 2014; Deloitte, 2014).

### 2.1.1.1. iPads

iPads are becoming popular to consumers. According to Deloitte (2014)'s survey and ClickCare (2014), Apple's Inc. is in control of the market: 54 percent of iPhone owners have an iPad while only six percent have a Samsung tablet. In fact, Apple's iPads sold over 14 million tablets in the year 2014, allowing them to maintain their position over other tablets running Android or Microsoft operating systems (Nguyen & Chaparro, 2011). Few IT leaders saw iPads as healthcare "game-changers," especially with the view of iPad EHR implementations as a way to promote useful compliance for physicians (ClickCare, 2014). The usage of iPads occur more rapidly than expected by IT professional specialist in healthcare; in result, iPad had accelerated EHR implementation.

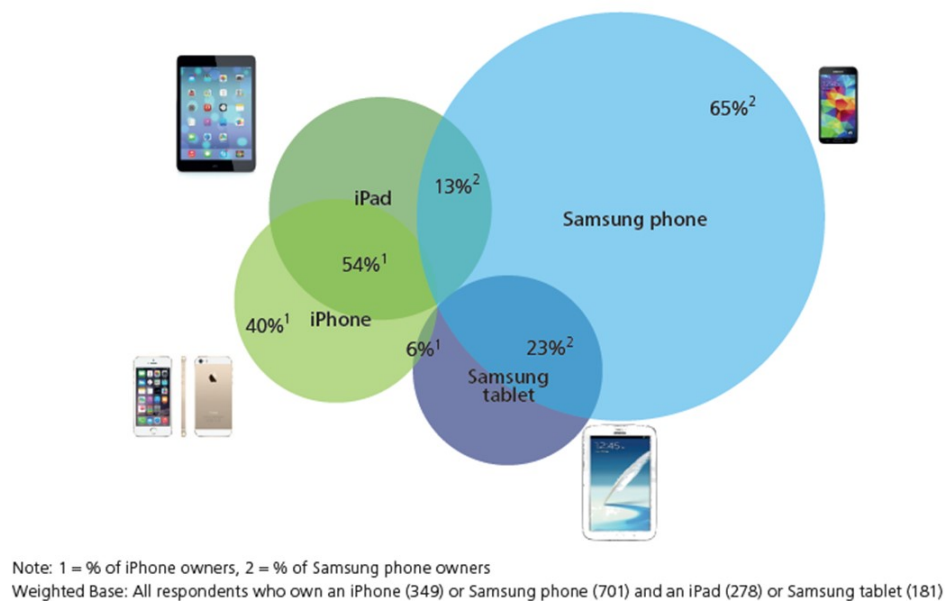


Figure 2.2. Android vs. Apple Ownership Comparison (ClickCare, 2014)

A possible problem for employee personnel using iPads within the work place are operating system and application software updates. The updates for iPads uses

iOS updates, which is an operating system manufacture by Apple Inc. protecting not only the device itself but also its data, and the entire ecosystem (Apple, 2015). This includes everything users do locally on networks and with various Internet services. If an employee is using an iPad that is suppose to be running on iOS 9.1, but is running iOS 8; this could possibly result into exploited vulnerabilities. Updates are issued to fix bugs that may have caused a problem before-hand with the previous iOS update. Apple had issued several updates over the years such as: iOS 7, iOS 8, and currently iOS 9.1.

iOS 4.2.1 was released on November 22, 2010 which added iPad compatibility - the beginning of the iPad updates. Using an issued iPad for work within the hospital should not cause many problems, because the technicians on-site will have access to install the necessary updates. In addition to mainting software updates, another possible problem is malware.

Malware is becoming an increasing threat for mobile devices. Malware is a malicious software use to disrupt an users PC, and can also be used for various malicious intent. For example, malware can be used to spy on the users browsing, collect sensitive data or carry out identity theft. There are many methods of deploying malware. For security purposes, Apple iOS devices allow users to install applications only from the Apple App Store as a security method. Apple Inc. reviews the application systemically (Felt, Finifter, Chin, Hanna, & Wagner, 2011). In addition to malware becoming a rising threat, theft is a high risk as well for iPads.

Devices can sometime result into theft. Sixty-four (64) percent of enterprise respondents reported that users devices containing sensitive data have been lost or stolen (Morrow, 2012). According to Apple's iOS 9.1 Software License Information (Apple, 2015):

*If your device is lost or stolen and you have "Find My iPhone" enabled, you can use "Find My iPhone" to attempt to suspend the ability to pay with the virtual credit and debit cards on the device by putting it into Lost Mode*

*(Apple, 2015).*

BYOD must be protected by HIPAA. Manufacturers who develop the devices, have protection schemes in place (Morrow, 2012). In today's society, firewalls are commonly used to conceal data from observation. Nearly every organization has a range of authentication as well as secure layers and transport layer security encryption (Morrow, 2012). Firewall protection is great to use as the a way to recover from a possible data breach incident. With employees using their own devices, this does create vulnerabilities. For instance, IT technicians check keyboards for key loggers and software for any known malware; yet, with outside devices entering the building, this carries different challenges (e.g ensuring the proper security software is install on the staff's privately own device). This can affect the organization because it could seriously put patients personal information at risk. The process of recognizing if an employees device is being targeted can be problematic. According to Morrow (2012)'s study, "Sixty-eight (68) percent said employees [within the health organization] have no way of identifying known mobile device vulnerabilities that could be affecting their network." Despite the potential risk involving of iPads, the budget for healthcare security and security training protect data breaches and security data vulnerabilities.

## 2.2 Budget

The U.S government allocated approximately 19 billion dollars a year in funding for programs to help healthcare providers implement EHR as part of the economic stimulus package enacted in February 2009 (Bardhan & Thouin, 2012). EHR has undoubtedly made an impact within the healthcare industry. The estimated net benefit from using an EHR system for a five-year period is 86,400 dollars per provider (Collum & Bisakha, 2015). Several studies have reported evidences of the positive impact of EHR on healthcare quality, including lower mortality rates, higher vaccination rates, and patient safety indicators (Bardhan &



Thouin, 2012). This is important for hospitals as it earns a valuable profit in return, just as a regular business does; however, with EHR records being interconnected, there have been several data breach reports coming in as the years pass by. Security breaches are concerns for electronic records just as lost or misplaced paper were previously. Under the Subtitle D-Privacy, Sec. 13400. Definitions in the HITECT Act;

*the term “breach” means the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information (HealthIT.gov, 2013)*

The value of health information security is increasing rapidly. With data breaches happening constantly, it is causing the economy to spend more money to increase security. These new penalties, ranging up to \$1.5 million, are linked to the severity of the violation; likewise, many states have implemented breach notification laws over the past decade (Kwon & Johnson, 2013). It is estimated that medical data breaches cost \$6.5 billion to the healthcare industry (Fowler, 2015). Figure 2.4 displays the total government spending leading up to a five year period.

The government spent \$1,096 billion in 2010 for healthcare; however, between the years 2011 to 2015, the amount of money spent had increased. The financial spending did decrease from 2011 to 2013; but there was a significant increase until 2014. According to the Figure 2.4, the spending for healthcare is expected to increase in the year 2016. In order to decrease the number of data breaches, national efforts to advance health IT have not adequately addressed privacy (McGraw et al., 2009).

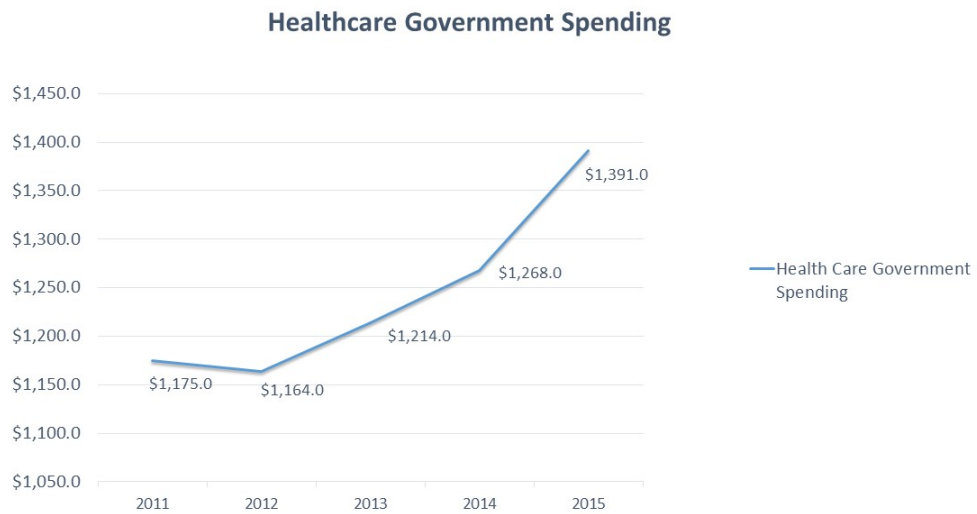


Figure 2.3. U.S Healthcare Total Government Spending (Five-Year Period) (Chantrill, 2015)

### 2.3 Government Guidelines

EHR are designed to be accessed easily from remote sites such as a clinic across town or even across the country. It is likely that data will be lost or misplaced. The Health Insurance Portability and Accountability Act (HIPAA) of 1996 amended a framework for privacy and security that requires compliance in transmission and disclosure of certain patient data (Taitzman, Grimm, & Agrawal, 2013). The sole purpose of the HIPAA Privacy Rule is to protect the privacy of individually identifiable health information (HHS.gov, 2011). According to Horowitz (2006), “privacy is inherently an ethical concept that is understood to represent something other than an individuals obligation to show and tell all” (Horowitz, 2006).

Even with HIPAA in place, there are few exploitations occurring; however, it has allowed, EHR managers become better prepared to handle the situation.

According to Redspin (2013), “one must think of IT security as a chronic illness, a condition that requires ongoing treatment, testing, and re-evaluation.” Exploitations will happen every so often, but that is how security analysts learn what vulnerabilities need to be addressed. The ongoing treatment and testing needed to make the security better is the purpose of Health Information Technology for Economic and Clinical Health Act (HITECT). HITECT Act was noted as Title XIII of Division A and Title IV of Division B of the American Recovery; the Reinvestment Act of 2009 (Pub. L 111-5) is mainly to provide a structure to protecting EHR (HealthIT.gov, 2009). According to the HITECT Act, it included the first federal data security breach notification requirements; in addition, it also required HHS to conduct HIPAA privacy and security audits (Solove, 2013). California enacted the first Security Breach Notification Laws (SNBL) in 2002 making the problem of inadequate information security in American business visible to the public for the first time (Winn, 2009).

The Department of Health and Human Service set an interim final rule explaining unsecured EHR. Unsecured EHRs are extremely dangerous; in fact, the Federal Register (Vol. 74 No.79, 2009) defines standards for data must be encryption. Encrypted data “the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key is in use today” (45 CFR 164 304, 2015). Cryptography cannot keep data information 100 percent safe, but it surely has a lower risk of data breaches. According to Redspin (2013), the existing HIPAA Security Rule reads:

*“Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(A) (1), including addressing the encryption/security of data stored in CEHRT in accordance with requirements under 45 CFR 164.312 (a) (2) (iv) and 45 CFR 164.306(d) (3), and implement security updates as necessary and correct identified security deficiencies as part of the providers risk management process for eligible hospitals” Redspin (2013).*

In technical terms, this statement from the existing HIPAA Security Rule gives hospitals the options on encrypting their data. According to Redspin (2013), an “addressable” requirement has the idea of something that is less than mandatory. However, the Federal government could fix that with one simple change to the HIPAA Security Rule. Redspin suggests that a certain hospital decide not to encrypt their data but may also it serve as a target.

#### 2.4 Breach Notification

When data could be possibly be at risk of a known employees must be trained myriad of information that could be used for malicious purposes. The breach notification provisions of Section 13402 apply to HIPAA covered entities and their business associates that access, maintain, retain, modify, record, store, destroy, or otherwise hold, use, or disclose unsecured EHR (Federal Register (Sections 13402 (a) and (b)) (Vol. 74 No.79, 2009). If a possible risk of data breach occurs, there is a breach notification requirement and must be reported to the Secretary.

According to HHS Breach Notification Rule, the covered entity must include a toll-free phone number that remains active for at least 90 days where individuals can learn if their information was involved in the breach. The toll-free phone number is a way that individuals can call to reach businesses without being charged for the call. The most common toll-free phone numbers used today are: 800, 888, 877, 855, and 844. Informing the media is similar to the informing the individual. When informing the media, the incident has to be notified no later than 60 days following the discovery of the data breach and has to include the same information mentioned to the individual when notified. After notifying the individual and media, the secretary is the next person to be notified. Security breaches affecting fewer than 500 individuals are to be notified to the secretary no later than 60 days; however, more than 500 individuals are to be notified without unreasonable delay (HHS.gov, 2011). In addition to notifying a breach, HHS has develop a formal

reporting process to the Office of Civil Rights. The Office of Civil Rights submission form is broken into five sections: covered entity, business associate, breach, notice of breach and actions taken, and attestation. There are two different forms: “Breaches Affecting 500 or More Individuals” and “Breaches Affecting Fewer than 500 Individuals.” It is imperative to notify the Secretary about the issue of discovered breach as mentioned in CFT Title 45, Subtitle A, Subchapter C, Part 164, Subpart D, 164.408:

*Standard. A covered entity shall, following the discovery of a breach of unsecured protected health information as provided in 164.404(a) (2), notify the Secretary.*

After the breach notification, patients are notified of the possible security risk situation, HIPAA included penalty fines (see Table 2.1) which are effective today. According to the Federal Register (Vol. 74 No. 209, 2009), the violations are defined in four tiers. The description of the tier violations are as followed:

- Tier 1 represents covered entity or individual did not know the act was HIPAA violation (Vol. 74 No. 209, 2009).
- Tier 2 represents having a reasonable cause and was not due to willful neglect (Vol. 74 No. 209, 2009).
- Tier 3 represents an incident that was due to willful neglect but the violation was corrected within the required time period (Vol. 74 No. 209, 2009).
- Tier 4 represents an incident that was due to willful neglect and was not corrected (Vol. 74 No. 209, 2009).

## 2.5 Summary

Due to many benefits, EHR is continuously expanding in today’s healthcare industry. Security threats are expanding to exploit vulnerabilities in EHR. BYOD

Table 2.1  
Parameters and Tier Violations

Tier	Penalty
Tier 1	\$100-50,000
Tier 2	\$1,000-50,000
Tier 3	\$10,000-50,000
Tier 4	\$50,000>

is now a key important aspect within healthcare. Various of government guidelines and acts are established to protect patients privacy and to set a security structure for EHR are all presently being use within hospital organizations. To protect patient information, healthcare spending on EHR had been increasing after the year 2012 and is expected to increase this year. Data breaches are hurting health organizations financially due to the level of data breaches. Data breaches are occurring through different aspects. It is important to determine if the BYOD policy serves as a risk possibly causing an increase of data breaches.

## CHAPTER 3. METHODOLOGY

The intent of this research was to determine if the BYOD policy could be a risk causing an increase in data breaches. To narrow the number of devices used by healthcare professional users, iPads was used by this exploratory research work.

This chapter describes the method of research and data collection; also, the flow diagram used to create the simulation model. Due to the nature of the research, the researcher was primarily focused on a qualitative study.

### 3.1 Theoretical Framework

A simulation model was created using AnyLogic software to compare wireless devices and desktop computer based on the nurse and doctor usage. With the focused hospital, Franciscan St. Elizabeth Health - Lafayette East Health included in the simulation model, the model was ran twice: once with the staff using iPads only thorough the clinic; secondly, with desktops. Employee computer practices including logging out, leaving desktop computers unattended, and advantage taken by the patient due to employee negligence. Based on both runs, a comparison was made to compare issues between the BYOD policy and desktop computers usage.

#### 3.1.1 AnyLogic

In order to accurately simulate the model to compare the security risk factors, AnyLogic served as the best option because it provided a simple way to model the EHR risk factors. In addition, AnyLogic is a risk-free method that cannot cause any damage to BYOD to test the methods within a health clinic.

System dynamics was used to create the simulation modeling. “The goal of systems thinking and system dynamics modeling is to improve our understanding of the ways in which an organizations performance is related to its internal structure and operating policies, including those of customers, competitors, and suppliers and then to use that understanding to design high leverage policies for success,” as mentioned by Sterman (2000).

### 3.2 Sample Set

The sample set used in the model considered of one nurse and doctor within the model in an ideal healthcare clinic office setting. The patients entered into the model was randomly generated based on an entrance rate, which is later define in the next chapter.

### 3.3 Testing Methodology

The flow diagram developed based on my ideal healthcare office, shown in Figure 3.1, served as the basis for creating the simulation model to test the methodology of the BYOD policy. Based on a eight hour work day (eight A.M to five P.M) excluding the one hour lunch break, within the clinic of Franciscan St. Elizabeth Health- Lafayette East, the average waiting time in the clinic and patients’ attention provided the model opportunities for data comprise.

Figure 3.1 shows the main parts of the model and the model setup screen via screen capture. The model began with the patient entering into the model. At the origin of the model, the patient entered based on the type of emergency. There is a split outcome of emergency or non-emergency entrance. If it is an emergency (bottom line), the patient was directed to the treatment room as quickly as possible and exit the model; however, if it is a basic check-up procedure for instance. The patient proceeded through the top line to registration. After the registration was completed, the patient waited in the rest area; meanwhile, the nurse prepared the



patient's EMR. On the first run, the model was ran with the nurse and doctor using only iPads; however, the second run consisted of using only desktop computers. The nurse and doctor worked on the patient's EMR from either a desktop or iPad. Afterwards, the nurse moved to the patient.

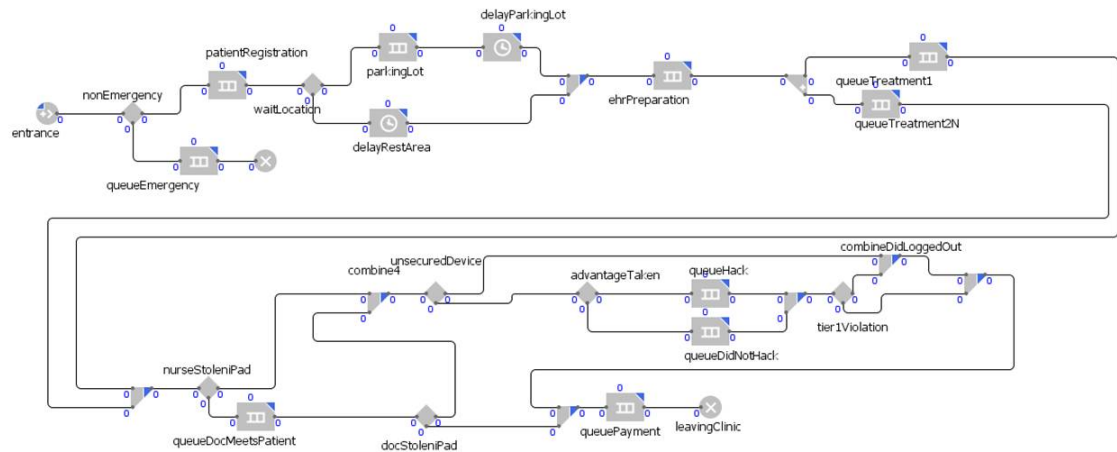


Figure 3.1. Simulation Flow Diagram

Once the nurse completed the patient's examination, there was an output for the nurse. Based on the first run (using wireless devices), the output consisted on whether or not the iPad was stolen while in the treatment room with the patient; in addition, whether or not the nurse and doctor signed out of the device resulted into a missing unsecured device. The second run consisted on whether or not the nurse and doctor left the desktop unattended while being with the patient; in addition, to whether or not the staff logged-out. The number of times the patient took advantage of the situation was another factor closely monitored. The threat of having a patient hacking into the clinic system also becomes another risk. As mentioned in Chapter 2, HIPAA has current tier violations which are in placed

today. To reduced the complexity, tier one violation (staff was not aware of the situation) was used in the model.

To calculate the risk of using iPads and desktop computers within the health clinic, the risk assessment method by (Cox Jr, 2008) was used:

$$\textit{Equation 1: Risk} = \textit{Threat} \times \textit{Vulnerability} \times \textit{Impact}$$

Based on the focus of the research, the threat of causing data breaches within the health clinic with the usage of iPads and desktops was compared. The vulnerability on the usage of both wireless and wired devices was provided by Bitglass (2014). To quantify the HIPAA tier violation one, the tier violations was used as a severity rate: one being the lowest severity, whereas, four being highest severity. Chapter D. Demonstrate Mathematics demonstrates how Equation 1 was used to calculate the risk of both BYOD and desktop computers. Once the risk was calculated, the patient's overall time from both model runs was recorded, averaged and compared.

The model was averaged using the fraction,  $\frac{\textit{risk}}{4}$ . The denominator, four, represented as the risk over the number of HIPAA tier violations. Given the average risk for both threats, average wait time, and total time of the clinic hours for a one-day period; the risk of data breach due to patient waiting time was calculated using the formula in Equation 2:

$$\textit{Equation 2: Risk of Time} = \frac{100}{(\frac{\textit{risk}}{4} * 480\textit{mins}) - (\textit{AverageWaitTime})}$$

### 3.4 Chapter Summary

This chapter covered the qualitative research framework and method used in the study, what was being tested, and research questions. It also discussed the logic of the simulation model used to determine which EHR method had the lowest risk.

## CHAPTER 4. PRESENTATION OF DATA

As describe in the previous chapters, the purpose of this study was to determine if the BYOD policy was becoming a liability risk within hospitals by comparing a wireless device to desktop computer together. The focus devices compared was iPads and desktop computers. To reduce the complexity, the researcher ran the simulation model with one nurse and doctor observing the risk when treating the patient.

### 4.1 Initial Inputs and Parameters

The initial setup for the simulation model used data input listed in Table 4.1. The model randomly generated an approximate of 2,700 patients based on the arrival rate. The arrival rate for the patient was set for one every ten minute; while the nurse and doctor arrive rate was set for one per minute. The variable, “Probability of Emergency” and choice of “Wait Location” was undetermined; therefore, it was measured as 0.3. In technical terms,  $\frac{3}{10}$  of the patients that entered the clinic was emergencies and in need of immediate medical assistance.

Table 4.1  
Model Parameters

Parameters	Numbers Used	Source
Wait time	24 minutes	(Groeger, Tigas, & Wei, 2015)
Misplaced Device	0.68	(McCarthy, 2014)
System hack	0.23	(Bitglass, 2014)
Mobile Device Insecurity	0.32	(Ponemon Institute, 2015)
Did not logout	0.70	(Ponemon Institute, 2015)
Tier 1	0.30	Center (2015)
Desktop unattended	0.70	(Ponemon Institute, 2015)

#### 4.2 Process

The model took a simple approach towards patients attempting to take advantage due to employee negligence within the clinic while using either wireless or wired devices. Employee negligence was used as whether the nurse or doctor logged out of their desktop and if the desktop was left unattended.

The model assumed that for every patient that entered the model, each was seen and examined by one nurse and doctor before the leaving the clinic. The model ran twice on an eight-hour day period to determine if the BYOD policy had a lowest risk factor than the usage of desktops.

#### 4.3 Recorded Data Collection

The results recorded from AnyLogic was solely based on the data taken from Table 4.1 (Model Parameters). The first model experiment (using iPads) was completed and displayed depending on the number of times the staff misplaced their iPad when examining the patient. This occurred three out of ten times. The iPad was not logged out one time out ten which resulted into an unprotected device.

Throughout the eight hour day, there was a one out ten times a patient took advantage of the misplaced, unprotected iPad.

The second model experiment (using desktops) was completed and displayed that the desktop was left unattended three out of ten times; in addition, seven out of ten time the staff did not logged out of the desktop. The advantage taken by the patient resulted into one out of ten times. Table 4.2 displays the results from AnyLogic simulation.

Table 4.2  
Model Results: Wireless vs. Wired

Table 4.3 Model Run 1: Wireless Device		Table 4.4 Model Run 2: Wired Device	
Model Experiment One	Occurrence	Model Experiment Two	Occurrence
Misplaced iPad	3 out of 10	Advantage taken	1 out of 10
Advantage taken	1 out of 10	Unattended desktop	3 out of 10
Unsecured device	1 out of 10	Did not logged-out	7 out of 10

The results from the simulation model was used by comparing the overall lowest risk involving each focused potential risk. Experiment one

The first model run generated a total of 2,659 patients within a eight hours period. There were 717 patients that choose to wait inside the clinic while others choose to wait in the parking lot before seeing the doctor while the nurses also prepare the patient medical record for the doctor usage. The second model run generated a total of 2,730 patients. Six hundred and eighty (680) patients choose to wait inside the clinic.

#### 4.4 Calculated Risk

To calculate the risk of BYOD and desktops, Table 4.5 displays the value used for the threat and vulnerability. As mentioned in Chapter 3, the researcher

focused on tier one violation. The quantified tier violation was used as the consequence within the risk equation.

Table 4.5  
Risk Value Input

Variables	Numbers Used	Source
Desktop threat	0.17	(HIMSS, 2015)
BYOD threat	0.29	(Ponemon Institute, 2015)
Vulnerability	0.48	(Bitglass, 2014)

Using the risk assessment equation, the risk for using iPads and desktop was calculated using only tier one violation; in addition, the vulnerability involving desktops and mobile devices potentially causing data breaches, according to Bitglass (2014). As mentioned in Chapter 3, Chapter D. Demonstrate Mathematics provides examples of how the risk was calculated. Table The calculated risk based on a tier one violation

Table 4.6 displays the calculated risk for desktops and iPads:

Table 4.6  
Risk Solutions

Threat	Tier 1
Desktops	8.16%
BYOD(iPads)	13.92%

The calculation for the risk of both desktop and iPads was used as the risk of a tier one violation.

Patients waiting in the treatment room also presented a risk. The average wait time in Franciscan St. Elizabeth Health - Lafayette East Health was 24 minutes (Groeger et al. (2015)). Given the risk of either BYOD or desktop, average wait time (24 minutes), and total time of the clinic business hours (8 hours = 480

minutes); the risk of data breach due to wait time was calculated using for formula:

$\frac{100}{(\frac{risk}{4} * 480mins) - (24minutes)}$ . Using iPads in the treatment room when treating the

patients resulted to 0.699; whereas, using desktops in the treatment room resulted to 1.353.

## CHAPTER 5. CONCLUSION

In conclusion, giving the increasing threats to IT infrastructure, the BYOD policy had a lower risk than using desktops within health clinics. Due to the results, the BYOD policy was not considered a liability risk. The focused BYOD, iPads, proved to have a lower risk compared to using desktop computer when treating patients. Using desktop computers within the treatment room had a summation risk of 20.4% compared to using iPads which had a summation risk of 34.8%. According to research, using wireless devices increases efficiency and flexibility when using EHR systems to update patient EMR compared to using desktop computers; however, the increase of data breaches was the main concern involving new policies and security measures.

The patient/employee wait time was easily calculated using the formula:  $\frac{100}{(\frac{risk}{4} * 480mins) - (AverageWaitTime)}$ . Franciscan St. Elizabeth Health - Lafayette East Health average wait time was used as the "Average Wait Time". The patient/employee wait time contributed a huge factor. Using iPads to prepare patients' EMR for the doctors usage when examining the patient resulted to a solution of 0.699; however, using a desktop computer resulted to a solution of 1.353. Uniquely, the summation risk for iPad was higher than the summation risk for desktops, but the risk of time when using iPad proved to be lower than desktops.

Comparing the risk when using iPads and desktops, the simulation model also proved iPads used within the clinic had a lower risk than desktops. The first run consisted of one nurse and doctor which both used an iPad to utilize patients' EMR in the clinic; unlike the second run, consisted the usage of desktop computers. The material needs was recorded after performing the two model runs. The focus of the simulation model was as followed: the number of times the nurse and doctor was victim of a stolen iPad, leaving the desktop unattended/unsecured device, and



potential opportunity taken by patient due to employee negligence. Based on the first run using iPads in the treatment room, the device was stolen three out of ten times during a typical work day. The number of times the nurse and doctor did not logged out resulting into an unsecured device occurred one out of ten times; in addition, one out of ten times the patient took advantage of the situation despite the occurrence of negligence's. Model run two consisted of three out ten times which the desktop computer was left unattended when treating patient. There was also an occurrence of seven out of ten forgotten to logged out of the computer. Despite the negligence, few patients took advantage of the situation two out of ten times.

The risk for the BYOD policy could possibly be lower if employee negligence were to decrease from 70%. Because of the increase of negligence caused by employees, it is recommended enacting an outcome of mandatory employee clinical re-training to reduce the employee negligence. Mandatory clinical training could possibly lower the risk of employee negligence which could cause a decrease of the BYOD risk. Also to decrease employee negligence, increasing communication through-out the clinic could help. Decreasing employee negligence could slightly reduce the government spending like-wised in the year 2012.

The model can be used in future research to test new IT equipment and policies within healthcare clinics. For example, a hospital could use the model to analyze whether or not patients are leaving without seeing the doctor due to emergency waiting. Research also needs to be performed to determine the risk factors and calculate the risk analysis in order to calculate the summation; emergency waiting time distribution; and understanding of HIPAA violations of specify incident. That research should also include a focused health clinic to include wait time. The research performed in this study demonstrated a possible liability risk factor used widely within clinics based on nine hour business day proving that the BYOD policy is not consider as a liability risk.

## APPENDICES

CHAPTER A. HEALTH CLINIC LAYOUT

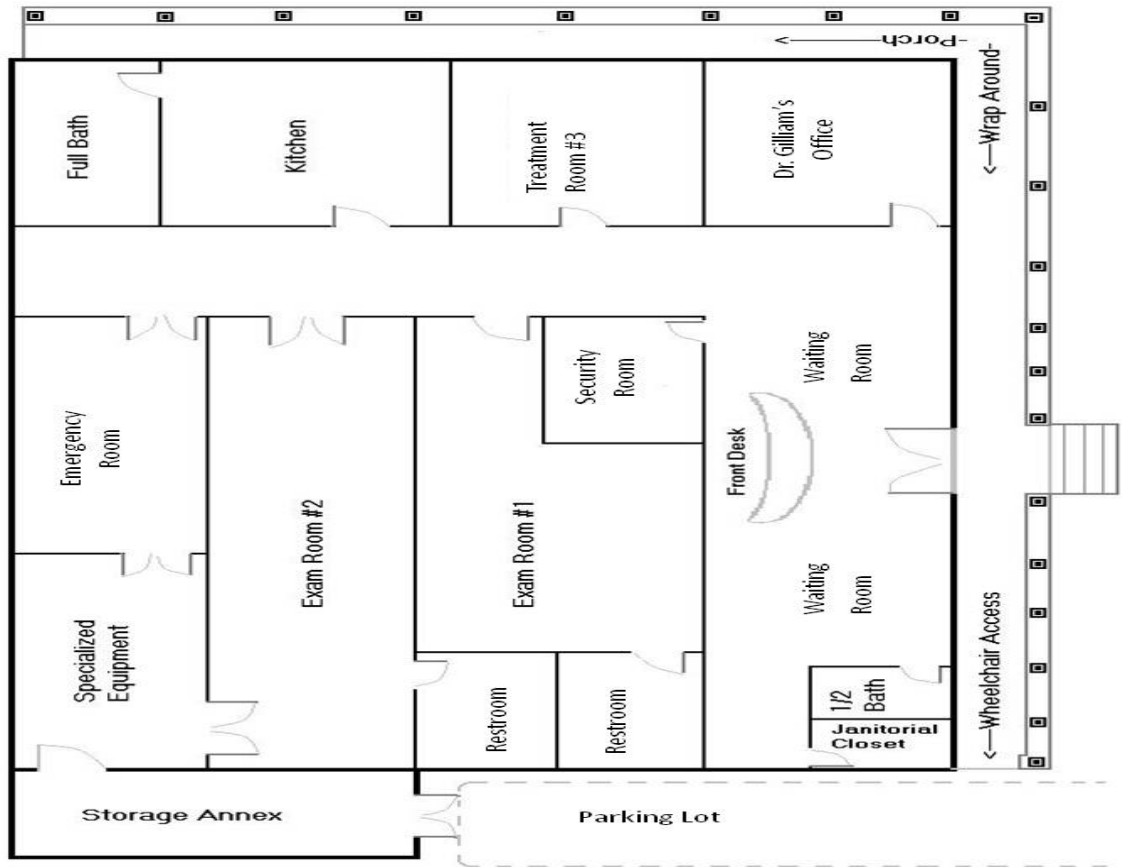


Figure A.1. Health Clinic Layout

CHAPTER B. BYOD SIMULATION MODEL

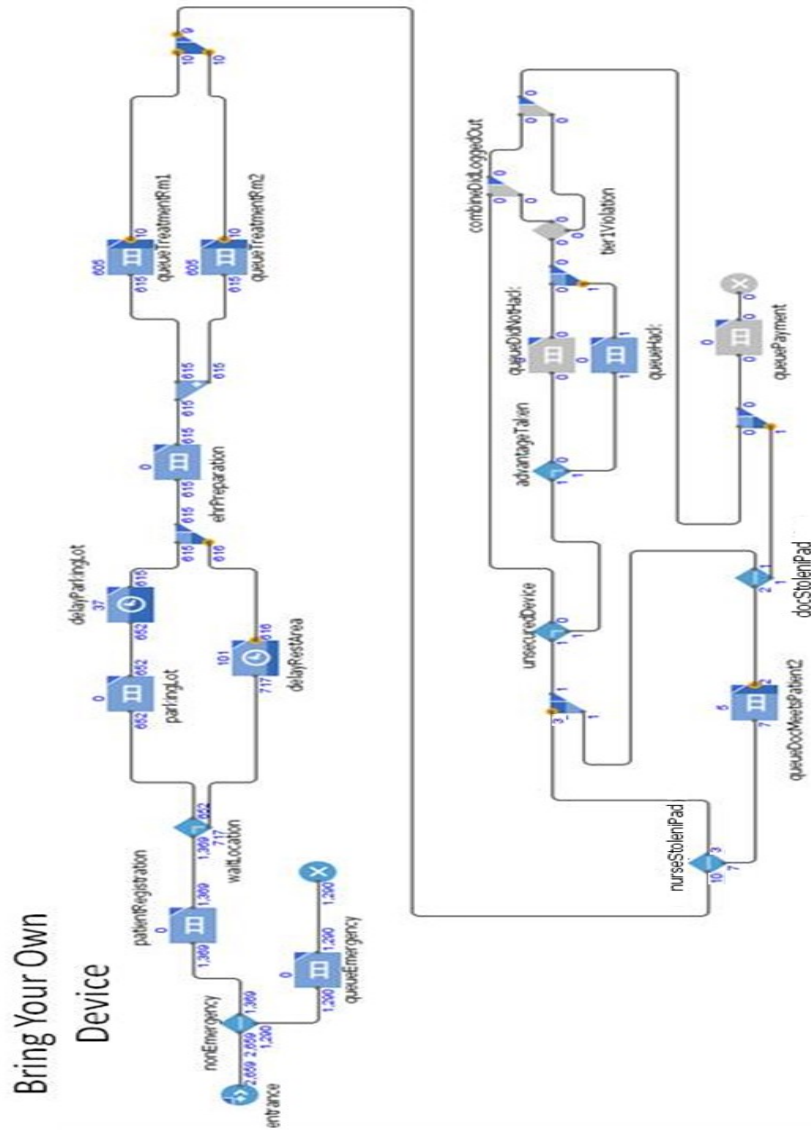


Figure B.1. BYOD Simulation Model

CHAPTER C. DESKTOP SIMULATION MODEL

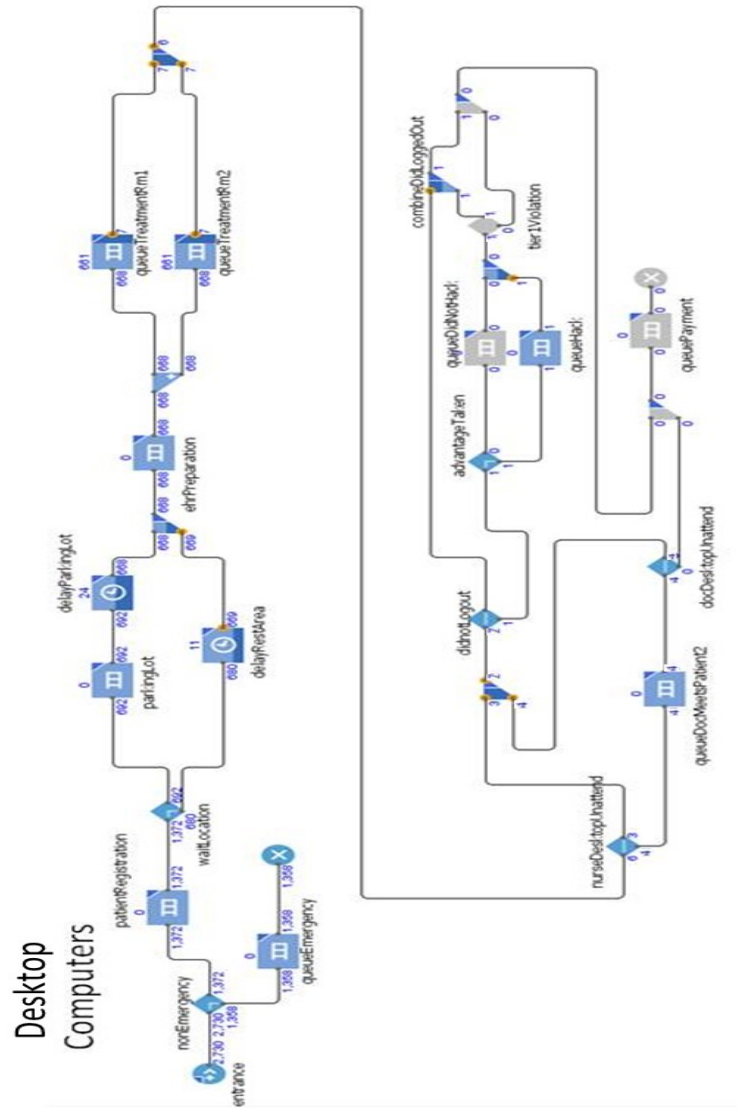


Figure C.1. Desktop Simulation Flow

## CHAPTER D. DEMONSTRATE MATHEMATICS

*Equation 1:* Risk = Threat x Vulnerability x Impact

Equation 1 was used to calculate the risk for using iPads and desktops within the health clinic. Example of how to use equation: according to (Ponemon Institute, 2015), the threat for using iPads is 29%. The vulnerability, 48% was used. Based on the impact, HIPAA tier violation one-four was used. The equation was set as the followed:

$$\text{Risk} = 0.29 \times 0.48 \times 1$$

$$\text{Equation 2: Risk of Time} = \frac{100}{\left(\frac{\text{risk}}{4} * 480 \text{mins}\right) - (\text{AverageWaitTime})}$$

Equation 2 was used to calculate the risk based on the time spent in the treatment room with personnel. With one hundred as the numerator, and the value of Equation 1 (the risk of either BYOD or desktop), multiplied by the 8 hour business day (converted into minutes = 480) subtracting the average wait time results in the risk based on time.

## LIST OF REFERENCES

## LIST OF REFERENCES

- 45 CFR 164 304, F. R. (2015). Guidance to render unsecured protected health information unusable, unreadable, or indecipherable to unauthorized individuals [Federal Register].  
doi: <http://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html>
- Apple. (2015). Apple's software license and agreements. In *ios 9.1, software license and agreements*.
- Bardhan, I. R., & Thouin, M. F. (2012). Health information technology and its impact on the quality and cost of healthcare delivery. [Journal Article]. *Decision Support Systems*, 55(2), 438-449. doi: 10.1016/j.dss.2012.10.003
- Bitglass. (2014). The 2014 bitglass healthcare breach report [Healthcare Breach Report].  
doi:  
[http://pages.bitglass.com/BR-Healthcare-Breach-Report-2016\\_PDF.html](http://pages.bitglass.com/BR-Healthcare-Breach-Report-2016_PDF.html)
- Center, D. (2015). Update: Privacy and security of protected health information [Healthcare Breach Report].  
doi: <http://www2.deloitte.com/content/dam/Deloitte/us/Documents/life-sciences-health-care/us-lshc-privacy-and-security.pdf>
- Chantrill, C. (2015). Fy budget data) [Budget Report]. *U.S Government Spending Details*.
- ClickCare, L. (2014). Healthcare byod and hipaa security: The issues and a solution.  
doi: [http://www.clickcare.com/pdf/iClickCare BYOD HIPAA Secure.pdf](http://www.clickcare.com/pdf/iClickCare%20BYOD%20HIPAA%20Secure.pdf)
- Collum, N., & Bisakha. (2015). does electronic health record use improve hospital financial performance? evidence from panel data [Healthcare Management Review].
- Cox Jr, L. A. T. (2008). Some limitations of risk= threat× vulnerability× consequence for risk analysis of terrorist attacks. *Risk Analysis*, 28(6), 1749–1761.
- Deloitte. (2014). Global mobile consumer survey [Survey].  
doi: <http://www2.deloitte.com/content/dam/Deloitte/nl/Documents/technology-media-telecommunications/deloitte-nl-tmt-global-mobile-consumer-survey-2014.pdf>



- Felt, A. P., Finifter, M., Chin, E., Hanna, S., & Wagner, D. (2011). A survey of mobile malware in the wild. In *Proceedings of the 1st acm workshop on security and privacy in smartphones and mobile devices* (pp. 3–14).
- Fernandez-Aleman, J., Senior, I., Lozoya, P., & Toval, A. (2013). *Security and privacy in electronic health records: A systematic literature review* (Vol. 46) [Generic]. doi: 10.1016/j.jbi.2012.12.003
- Filkins, B. (2015). Health care cyberthreat report [Report]. *SANS White Analyst Whitepaper*.
- Fowler, S. M. (2015). Measuring the correlation between risk knowledge and comfort utilizing on-line medical data.
- Granger, S. (2001). Social engineering fundamentals, part i: hacker tactics. *Security Focus, December, 18*.
- Groeger, L., Tigas, M., & Wei, S. (2015). Er wait watcher.  
doi: <https://projects.propublica.org/emergency/hospital/150109>
- Hayrinen, K., Saranto, K., & Nykanen, P. (2008). *Definition, structure, content, use and impacts of electronic health records: A review of the research literature* (Vol. 77) [Generic]. doi: 10.1016/j.ijmedinf.2007.09.001
- HealthIT.gov. (2009). American recovery and reinvestment act [Article].  
doi: <http://www.healthit.gov/sites/default/files/hitechactexcerptfromarawithindex.pdf>
- HealthIT.gov. (2013). Guide to privacy and security of health information. chapter 3: 10 step plan for meeting privacy and security portions of meaningful use [Article].  
doi: <http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide-chapter-3.pdf>
- HHS.gov. (2011). Risk management plan [Article].  
doi:  
<http://www.phe.gov/about/amcg/toolkit/documents/risk-management.pdf>
- HIMSS. (2015). Transforming health through it [HIMSS Asia Pacific Exclusive Article].
- Horowitz, I. L. (2006). Privacy, publicity and security: the american context. privacy is not only a right but also an obligation [Journal Article]. *EMBO reports, 7 Spec No*, S40.
- Kierkegaard, P. (2011). Electronic health record: Wiring europe's healthcare. *Computer Law & Security Review, 27(5)*, 503–515.
- Kwon, J., & Johnson, M. E. (2013). Security practices and regulatory compliance in the healthcare industry [Journal Article]. *J. Am. Med. Inf. Assoc., 20(1)*, 44-51. doi: 10.1136/amiajnl-2012-000906

- McCarthy, K. (2014). Study: Majority of healthcare breaches due to theft.  
doi: <http://www.nuemd.com/news/2014/11/13/study-majority-healthcare-data-breaches-due-theft>
- McGraw, D., Dempsey, J., Harris, L., & Goldman, J. (2009). Privacy as an enabler, not an impediment: Building trust into health information exchange [Journal Article]. *Health Aff.*, *28*(2), 416-427. doi: 10.1377/hlthaff.28.2.416
- Morrow, B. (2012). Byod security challenges: control and protect your most sensitive data. *Network Security*, *2012*(12), 5–8.
- Nguyen, B., & Chaparro, B. (2011). iPad usage patterns on-the-go and at work. *Usability News*, *13*(2).
- Nigrin, D. J. (2014). When 'hacktivists' target your hospital [New England Journal of Medicine].
- Perakslis, E. D. (2014). *Cybersecurity in health care* (Vol. 371) [Generic]. doi: 10.1056/NEJMp1404358
- Ponemon, I. (2013). Third annual survey on medical identity theft [Report].
- Ponemon Institute, L. (2015). Fifth annual benchmark study on patient privacy data security.
- Redspin, I. (2013). *Annual breach report 2013* [Report].
- Solove, D. J. (2013). Hipaa turns 10: analyzing the past, present, and future impact.
- Sterman, J. D. (2000). *Business dynamics: systems thinking and modeling for a complex world* (Vol. 19). Irwin/McGraw-Hill Boston.
- Taitsman, J. K., Grimm, C. M., & Agrawal, S. (2013). *Protecting patient privacy and data security* (Vol. 368) [Generic]. doi: 10.1056/NEJMp1215258
- Vol. 74 No. 209, F. R. (2009). Rules and regulations [Federal Register].
- Vol. 74 No.79, F. R. (2009). Rules and regulations [Federal Register].
- Winn, J. K. (2009). Are "better" security breach notification laws possible?(symposium: Security breach notification six years later) [Journal Article]. *Berkeley Technology Law Journal*, *24*(3), 1133-1165.
- Wright, C. (2004). Top three potential risks with outsourcing information systems. *Information Systems Control Journal*, *5*, 40–42.