SECURITY, PRIVACY, CONFIDENTIALITY AND INTEGRITY OF EMERGING HEALTHCARE TECHNOLOGIES: A FRAMEWORK FOR QUALITY OF LIFE TECHNOLOGIES TO BE HIPAA/HITECH COMPLIANT, WITH EMPHASIS ON HEALTH KIOSK DESIGN

by

Harold Kwabena Takyi

Bachelor of Science Degree in Information Technology & Management, Point Park University,

2005

Master's Degree in Health Information Systems (RHIA Option), University of Pittsburgh, 2008

Submitted to the Graduate Faculty of

The School of Health and Rehabilitation Sciences in partial fulfillment

of the requirements for the degree of

Doctor of Philosophy

University of Pittsburgh

2018

UNIVERSITY OF PITTSBURGH

SCHOOL OF HEALTH AND REHABILITATION SCIENCES

This dissertation was presented

by

Harold Kwabena Takyi

It was defended on

November 13, 2018

and approved by

Judith T. Matthews PhD, MPH, RN
Research Associate Professor of Nursing, Associate Director, Gerontology Program, University Center for Social and Urban Research, University of Pittsburgh

Lauren Terhorst, PhD
Associate Professor, School of Health and Rehabilitation Sciences, Department of Occupational Therapy and School of Nursing, Department of Health and Community Systems, University of Pittsburgh

Mervat Abdelhak PhD
Associate Professor, Department of Health Information Management, University of Pittsburgh

Dissertation Advisor

Valerie Watzlaf, PhD, RHIA, FAHIMA
Vice Chair of Education and Associate Professor, Department of Health Information Management, University of Pittsburgh

SECURITY, PRIVACY, CONFIDENTIALITY AND INTEGRITY OF EMERGING HEALTHCARE TECHNOLOGIES: A FRAMEWORK FOR QUALITY OF LIFE TECHNOLOGIES TO BE HIPAA/HITECH COMPLIANT, WITH EMPHASIS ON HEALTH KIOSK DESIGN

Harold Kwabena Takyi, PhD

University of Pittsburgh 2018

This dissertation research focused on the following:

1. Determined possible vulnerabilities that exist in multi-user kiosks and the computer systems that make up multi-user kiosk systems.
2. Developed an evaluation system and audit checklist for multi-user kiosk systems adapted from the Office for Civil Rights (OCR) audit protocols, to address the vulnerabilities identified from our research.
3. Improved the design of a multi-user health kiosk to meet the HIPAA/HITECH standards by incorporating privacy and security (P&S) policies.
4. Explored the feasibility and preliminary efficacy of an intervention to explore the magnitude of differences in users' perceived risk of P&S breaches as well as the correlation between perceived risk and their intention to use a multi-user health kiosk.

A gap analysis demonstrated that we successfully incorporated 91% of our P&S polices into the design of a health kiosk that is part of an ongoing, large-scale investigation. This is higher than our initial target of 50%.

Repeated measures ANOVA was performed to analyze baseline and six-month follow-up of 36 study participants to measure the magnitude of the change in their perceived risk in response

to varied intervention approaches: usual care vs. printed materials vs. printed materials plus brief oral explanation. Results from the ANOVA revealed no significant group-by-time interaction (Time*Group) F (2, 33) = .27, p=.77, ηp2=.02, a significant main effect of time F (1, 33) = 4.73, p=.04, ηp2=.13, and no significant main effect of group F (2, 33) =1.27, p=.30 ηp2=.07.

Users' "perceived risk lessened over time (baseline and six-month follow-up), although the magnitude of the change was small. We were, however, unable to perform the correlation analysis as originally proposed because all kiosk participants included in the analysis intended to use the kiosk both at baseline and at six-month follow-up.

These findings may inform future research into methods aimed at reducing perceived risk of P&S breaches and using education and communication to reduce risky behavior by both internal and external users of new health IT applications and technologies. The findings may also provide a framework to guide policy in P&S of health applications, technologies and health IT systems.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

PREFACE

I extend my profound gratitude and acknowledgement to my advisor Dr. Valerie Watzlaf, PhD, RHIA, FAHIMA, for her guidance, thoughtfulness, patience, and support throughout my graduate studies and research. Special thank you and appreciation to Dr. Judith T. Matthews, PhD, MPH, RN, for allowing me to be part of the kiosk project team and to access the kiosk to run my study for this dissertation. I also thank Dr. Lauren Terhorst, PhD, for the tremendous help and guidance for the study design, development and statistical analysis of my dissertation. My acknowledgement also goes out to Dr. Mervat Abdelhak, PhD, for all the pieces of advice she gave me throughout my graduate studies and dissertation. A special thank you to the kiosk project team for all their help and support during the data collection process of my research work.

Finally, I would like to extend my sincere gratitude to my wife and kids for their support as well as bearing with my grumpiness during my graduate studies. Last, but not the least, a special shout out to my parents, my mother Comfort Amoah Bonse (RIP) and dad Christopher Kwabena Bonse for the support they have given me throughout my life.

1.0 INTRODUCTION

Recent increases in information security and privacy (P&S) breaches have led to more interest in and scrutiny of information security issues (Bui, Wang, & Clemons, 2017; Conti, Dehghantanha, Franke, & Watson, 2018). Regulators, security experts, technology developers and academic researchers are clamoring to find better ways to protect information (Angst, Block, D'Arcy, & Kelley, 2017; Bui et al., 2017; Sezgin, Yıldırım, Yıldırım, & Sumuer, 2018). Criminological reports about motivation and decision making among burglars found that offenders are deterred if there are signs indicating the presence of an alarm system or a dog (Angst et al., 2017). In information technology (IT) security/privacy, the signals could be in the form of policies (security education, training, and awareness [SETA] programs), monitoring and detection technologies (Angst et al., 2017; Kafali, Jones, Petruso, Williams, & Singh, 2017). Privacy and security policy development is an important part of developing secured technology (Kafali et al., 2017). This dissertation focused on P&S policy development as part of the systems/technology development cycle to mitigate privacy and security breaches.

The Technology Acceptance Model (TAM) was developed by Freed Davis in 1980 to study factors that influence acceptance of computer technology (Ahlan & Ahmad, 2015). One variable that has been added to the extension of TAM is "perceived risk," which had been identified in many studies as one of the primary drivers of technology acceptance by users (Mitzner, Stuck,

Hartley, Beer, & Rogers, 2017). Privacy, security and confidentiality are the main variables that have been used to define "perceived risk"(C.-F. Li, 2013). In this dissertation we will be using "perceived risk" to mean perceived risk of breach of P&S. The findings provide P&S guidance for the development and deployment of multi-user kiosks and for the education and training of kiosk developers.

There have been numerus exploratory studies into the P&S of information technology, and computer systems. However, there have not been many experimental, and well controlled studies into privacy, security and confidentiality of various IT systems, especially in the Health IT arena (Merete Hagen, Albrechtsen, & Hovden, 2008). Researchers have the responsibility to conduct well-designed studies that shed light on this very important issue of P&S as new technologies are developed. A pilot study conducted as part of this dissertation examined the feasibility of conducting a randomized controlled trial to determine users' perceived risk associated with a novel health IT and whether such perceptions affected their intention to use the technology over time.

1.1 SPECIFIC AIMS

1.1.1 Specific aim 1

There is very limited literature on the development of P&S policies for health applications. P&S is usually an afterthought in the system development lifecycle, as is evidenced in recent high-profile breaches. This dissertation developed P&S policies, aligned with the OCR audit protocol,

during development and deployment of a multi-user health kiosk, to make sure it was HIPAA/HITECH compliant.

1.1.2 Specific aim 2

Recent high-profile data security breaches have shown that more attention must be paid to users (both internal and external users) when developing P&S policies if we are to succeed in our fight against this menace. There have been very few empirical, randomized controlled trials (RCTs) investigating "perceived risk" and how it affects "intention to use" health IT systems. This research focus could go a long way to help shape polices, training and communication of P&S policies. This dissertation explored the feasibility and preliminary efficacy of an intervention to reduce users' "perceived risk" of P&S breaches and examined their intention to use a multi-user health kiosk.

2.0 BACKGROUND

Advances in computer technology have opened up a new frontier in the delivery of care to patients. Recent findings have shown widespread use of mobile devices and other computer technologies across the world. There has been an urgent need or "rush" to harness the power and other benefits of these technologies to provide healthcare services to patients (Gallagher, 2012; Kate & Borten, 2010; Sezgin et al., 2018).

For example, data from the Healthcare Information and Management Systems Society (HIMSS) show that 90% of the world's population has access to some sort of wireless signal. There are 5 billion cell phone users in the world, 70% of whom are in third world countries. Fifty percent of all cell phone users have access to the web through their cell phones, and over 100 countries currently use a form of mobile health technology. A report on the Healthcare IT News website shows tremendous movement to integrate different computer technologies into healthcare. Some of the items and processes mentioned are cloud-based systems, telemedicine, integration or genomic and predictive modeling to improve personalized medicine and empowering the increasingly demanding patient. Further, it has been estimated that the patient portal market will grow from $279.8M to about $900M, an increase of about 221%, through 2017 (Ratchinsky, 2014). P&S is a primary concern.

Another issue that has spurred the adoption of EHRs is the American Recovery and Reinvestment Act (ARRA), a US government mandate for all US hospitals to have had EHRs in place by the year 2015 (Blumenthal, 2009). To expedite implementation of the mandate, the government has provided incentives for the adoption of EHRs. These have included about $17

billion in financial incentives since 2011 for doctors and healthcare providers who use EHRs. Payments reached as much as $18,000 in the first year for the adoption of EHRs between 2011 and 2012, $15,000 for those who adopted EHRs in 2013, and a lower amount for those who adopted EHRs by 2014 (Blumenthal, 2009). Health Information Technology for Economic and Clinical Health (HITECH) legislation also threatens financial penalties to encourage the adoption of EHRs. Physicians who were not using EHRs by 2015 could lose 1% of their Medicare fees, followed by 2% in 2016, and 3% in 2017. Hospitals that did not comply by 2015 also faced penalties (Blumenthal, 2009). The spread of value-based healthcare and Medicare Access and CHIP Reauthorization Act of 2015 (MACRA) further announced these incentives and penalties as it has compiled quality reporting, value-based care and EHR incentive programs into one single system called the Merit-based Incentive Payment System (MIPS).

Stolen medical records are said to be worth about twice as much as other stolen records, including social security numbers, on the underground market (Robertson, 2013). Information on KevinMD.com, a reputable online journal, states that medical records sell for around $60 a copy (Kevin, 2007). An article in the online version of the New York Post on September 25, 2014, stated that medical information is worth 10 to 20 times more than credit card numbers on the underground market. Cyber criminals are said to be increasingly targeting the U.S. healthcare industry because they see the healthcare systems as a soft target (Kevin, 2007; Reuters, 2014). This is in part because healthcare providers are always the last to adopt new technologies and are often over-reliant on old legacy systems that mostly do not meet the P&S standard of today's sophisticated computer networks (Reuters, 2014). Some of these computer systems are not only old but have not been updated with the latest security patches. According to an annual survey on data protection policy by the Ponemon Institute, (an independent research group focused on privacy, data protection, and

information security policy), the proportion of healthcare organizations that have reported criminal cyber-attacks rose from 20% in 2009 to 40% in 2013, and it is expected to increase in the coming years (Paul III, Spence, & Bhardwa, 2018; Reuters, 2014).

Healthcare technology developers and providers are mostly interested in their bottom line and hence P&S has traditionally been an afterthought (Mitzner et al., 2017). Lack of funding and staffing for information security and inadequate investment in technology remains a problem in the healthcare sector (Gordon, Fairhall, & Landman, 2017). The type of question that most healthcare providers have had to answer is whether to invest in a new MRI machine which can bring in thousands of dollars every year, or to invest in a new firewall system (Reuters, 2014). Theft of EHRs is therefore a very lucrative business and bound to attract the interest of hackers who seek to profit from the sale of stolen medical records.

The actual cost of medical records theft to victims is, however, not monetary. Medical records are usually sold to people who lack medical insurance and hence cannot afford the cost of treatment for an ailment. The victim's information is used to obtain care, and in the process the user taints the victim's health record with diagnoses, prescriptions, and other information that could affect the victim when he or she seeks treatment in the future. For example, victims of healthcare fraud have had their premiums go up for conditions they do not actually have. Some have even been given the wrong medication because someone else had used their information to seek treatment. Other victims have been sent bills for treatments they did not receive (Kevin, 2007). Some stolen medical records have been sold to companies that sell healthcare products like testing supplies for diabetes. Such companies can then become a source of constant harassment to the victims whose health records were stolen(Kevin, 2007).

Recent increases in high profile information security/privacy breaches and the manner in which the breaches occurred means this issue has to be tackled throughout the systems/technology development lifecycle (Kafali et al., 2017; Sharma et al., 2018; Takyi, Watzlaf, Matthwes, Zhou, & DeAlmeida, 2017). It is reported that 90% of organizations have had to deal with a security issue in one year (Siponen, Pahnila, & Mahmood, 2007). A 2017 survey of US companies with more than 500 employees found that 90% of the companies had cybersecurity polices. Yet only two-thirds (66%) of the companies enforced those policies and hence were vulnerable to attacks (Kemper, August 31, 2017).

2.1 RESEARCH PROBLEM

Even though emerging healthcare technologies provide tremendous benefits in terms of cost and convenience to patients and healthcare providers, there are various P&S and confidentiality issues that need to be addressed (Harman, Flite, & Bond, 2012; Peterson & Watzlaf, 2015; Yüksel, Küpçü, & Özkasap, 2017). The increased adoption of emerging healthcare technologies is set to increase P&S and confidentiality issues as more people try to exploit the vulnerabilities of systems (Adhikari, Richards, & Scott, 2014; Gunter & Terry, 2005; D. G. O'Brien & Yasnoff, 1999; Papageorgiou et al., 2018). This ever increasing threat to P&S has made it more important to put systems and procedures in place that address both internal and external threats to patient data (Lewis, 2014; F. Li, Zou, Liu, & Chen, 2011). A 2017 survey conducted by the Ponemon Institute found that 90% of health care organizations/providers have had a data breach. Sixty-four percent

of these organizations reported a successful attack involving medical files in 2016 (Gordon et al., 2017).

Growing concerns over healthcare information P&S have brought about expansion of healthcare regulations like the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) to safeguard patient data/information. These concerns have also resulted in an overhaul of the P&S requirements necessary to achieve compliance as well as a tremendous increase in fines for noncompliance (J. Kwon & Johnson, 2013). Further, a new regulation by the European Union entitled the General Data Protection Regulation (GDPR) was enforced in May 2018 and includes stringent rules on the use, transmission and processing of personally identifiable information.

Research has shown that perceived risk is an important determinant of technology acceptance and usage (Blumenthal, 2009; C.-F. Li, 2013; H. Li, Gupta, Zhang, & Sarathy, 2014; Mitzner et al., 2017). Curran and Meuter found that risk plays an important role in the intention to use, which then translates into actual usage when it comes to self-service technologies like clinical kiosks. This is because self-service technologies are "low touch" (with little or no human interaction) (Curran & Meuter, 2005). A recent study into concerns of Televideo technologies showed that users were more concerned with P&S when it comes to technology acceptance than other factors such as ease-of-use and benefit (Mitzner et al., 2017). Hence, developers of health applications must take the necessary steps to ensure that they develop private and secure systems that protect the user.

Evidence-based medicine is the integration of individual clinical expertise with best available external clinical evidence from systematic research for diagnosing and treating patients (Sackett, 1997). This can also be applied in P&S of health technology by showing evidence that

users are increasingly interested in P&S of health technology, applications and systems. This can serve as a strong incentive to improve P&S of the various health technologies, applications and systems. Organizations and decision makers will take P&S seriously if they are made aware through good research that users will not patronize their facilities if the P&S of their information cannot be assured or guaranteed (they stand to lose income that way).

2.2 OBJECTIVES OF THE STUDY

Research was done as part of this dissertation to:

1. Determine possible vulnerabilities that exist in multi-user kiosks and the computer systems that make up multi-user kiosk systems.
2. Develop an evaluation system and audit checklist for multi-user kiosk systems adapted from the Office for Civil Rights (OCR) audit protocols to address the vulnerabilities identified from our research.
3. Develop P&S policies and guidelines for multi-user health kiosk systems by adapting the OCR audit protocol.
4. Improve the design of a multi-user health kiosk to meet the HIPAA/HITECH standards by incorporating P&S policies.
5. Explore the feasibility and preliminary efficacy of an intervention to explore the magnitude of differences in users' perceived risk of privacy and security breaches as well as the correlation between perceived risk and their intention to use a multi-user health kiosk.

Findings in this dissertation could serve as a framework to drive policy in P&S of health applications, technology and health IT systems.

2.3 SIGNIFICANCE OF THE STUDY

There is increased concern among many healthcare providers about how to be compliant with P&S regulations when using health technologies (Kafali et al., 2017; Peterson & Watzlaf, 2015; Takyi, Watzlaf, Matthwes, et al., 2017). HIPAA and HITECH rules do not explicitly state the steps that organizations need to perform to become compliant with these technologies (tele-health, mobile-health, social media, and health kiosks). Hence, interpretation of HIPAA and HITECH rules remains a major headache for some healthcare organizations (Kafali et al., 2017; Lent, Zelano, & Lane, 2013; V. J. Watzlaf, Moeini, & Firouzan, 2010). This dissertation has explored computer security, information privacy, and confidentiality in relation to HIPAA and HITECH in non-traditional types of emerging healthcare technologies such as a multi-user health kiosk. The Office for Civil Rights (OCR) audit checklist then guided development of P&S and confidentiality procedures that should be used in such healthcare technologies. This approach will ultimately help healthcare providers to develop the appropriate P&S policies to secure such mobile health IT systems to achieve HIPAA and HITECH compliance.

This approach was utilized from the outset as part of the process of developing a multi-user health kiosk system with our collaborators from the University of Pittsburgh and Carnegie Mellon University. The resulting multi-user health kiosk was deployed at convenient community centers to target older adults, for helping them to manage various aspects of their health. The multi-

user health kiosk enables assessment and tracking of blood pressure and pulse rate, weight, oxygen saturation, and grip strength, and it provides interventions pertaining to self-management of health and chronic disease including patient-provider communication, sleep, bladder control, mobility and balance, lifestyle (nutrition, weight, and physical activity), and mood. Aspects of the OCR audit checklist were adapted to develop P&S policies to be implemented in the kiosk. The audit checklist formed the foundation upon which the multi-user health kiosk was secured. Applying the P&S policies across the multi-user kiosk architecture will help it to meet HIPAA and HITECH requirements.

Developing a secure system can lead to improvements in "perceived risk" by the user, which can lead to an increase in the user's trust of the system (such as a multi-user health kiosk), intention to use it, and actual use of the system (Curran & Meuter, 2005; P.-J. Hsieh, 2015; Kafali et al., 2017; C.-F. Li, 2013; Mitzner et al., 2017). Kiosk users' perception of risk regarding security, privacy, and confidentiality pertaining to use of a multi-user health kiosk was assessed for change over a 6-month period. Data were collected using an investigator-developed, paper-and-pencil questionnaire that elicited user response to "perceived risk" of P&S breaches and "intention to use" pre- and post-intervention in a randomized controlled trial of approaches designed to affect these perceptions.

3.0 LITERATURE REVIEW

3.1 INTRODUCTION

Protection of health information must be performed while complying with different health regulations such as HIPAA, HITECH, and other state and federal regulations. With advancement in electronic healthcare, personal health information can be entered, processed, stored, and transmitted electronically. This has uncovered numerous challenges to protecting an individual's privacy and to securing the tremendous amount of data generated. With the increased use of new and divergent technologies in healthcare, risks posed to users' information are at an all-time high. According to information from the OCR website, HIPAA complaints are soaring. Data breaches in 2017 surpassed previous years (Ziskovsky, 2017). According to data released by OCR, as of July 2017, approximately 174,792,250 people had been affected by 1,996 HITECH breaches. Business Associates accounted for 409 of the breaches, affecting approximately 31,239,362 people. The number of complaints by June 30, 2017 were 158,834, with a monthly average of 2,000. This was a significant increase compared to an average of 1,500 per month in 2015 and 1,750 in 2016. Most of the complaints focused on:

- Impermissible use and disclosure of protected health information (PHI)
- Lack of safeguards of PHI
- Lack of patient access to their PHI
- Use or disclosure of more than the minimum necessary PHI

- Lack of administrative safeguards of ePHI

Theft of information was the leading cause of all the breaches reported (Kafali et al., 2017). Unauthorized access accounted for 149 of the breaches. Laptop theft was the leading medium, responsible for more than 270 breaches. Hence, steps should be taken to understand the diverse healthcare rules as they relate to health information P&S, to create efficient ways to protect PHI both at rest and in transmission to be compliant.

3.2 HIPAA/HITECH RULES AND OTHER REGULATIONS

The need to protect patients' data and privacy gave birth to HIPAA and later to HITECH, which is a more detailed extension of HIPAA that deals with data security and privacy issues in an electronic environment. HIPAA/HITECH requires that all breaches affecting fewer than 500 people be reported to the individuals within 60 days and to the Department of Health and Human Services (DHHS) annually. Any breach involving more than 500 patients shall be reported to the affected individuals, media houses, and DHHS within 60 days (OCR, 2013; Ziskovsky, 2017). Many of these breaches could be avoided by combining good IT P&S practices with policies adopted from HIPAA/HTECH and other P&S legislation. These breaches are on the increase, but they can be mitigated. This is evident by the summary provided on the OCR website regarding the top reasons for all major breaches (see Tables 1 and 2).

Table 1: Top Reasons for All Major HITECH Act Breaches 2017

Top Reasons for All Major HITECH ACT Breaches as of July 2017

# of Breaches	Reason for Breach
627	Theft
419	Unauthorized Access/Disclosure
91	Loss
45	Improper Disposal
256	Hacking/IT incident

Source: HIPAA/SA Analysis of OCR Data

Table 2: Top Reasons for All Major HITECH Act Breaches 2014

Breaches Involving Network Services as of Feb. 17, 2014

# of Breaches	**Reason**
63	Unauthorized Access/Disclosure
57	Hacking/IT Incident
25	Theft

Source: HIPAA/SA Analysis of OCR Data

HIPAA was enacted in 1996 and amended in 2013. There are two major parts to HIPAA. The first part is to prevent individuals, especially those with preexisting conditions, from losing insurance coverage when they change jobs. The second part deals with creating standards for electronic data exchange, which also deals with the P&S of patient data (Choi, Capitan, Krause, & Streeper, 2006; Murphy, Gainer, Mendis, Churchill, & Kohane, 2011; Peterson & Watzlaf, 2015; Schachat, 2003; D. Solove, 2013). There are three major groups or covered entities (CE) that are

covered by HIPAA: health plans (e.g., managed care organizations), healthcare clearinghouses (e.g., billing companies, community health management information systems), and healthcare providers (e.g., healthcare facilities, doctors, nurses, therapists, etc.) (Choi et al., 2006; Kafali et al., 2017; Peterson & Watzlaf, 2015; D. Solove, 2013).

Noncompliance with HIPAA can lead to severe consequences for CEs. The most severe consequence is a fine of up to $250,000 and up to 10 years of imprisonment if the intent is to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious purposes (Annas, 2003; Choi et al., 2006). This fine has been increased from $250,000 to $1.5 million with the new HITECH rule.

The privacy rule of HIPAA was enacted to put in place a national standard for the flow of sensitive PHI. This is applicable to PHIs that are in oral, written, and electronic format. It governs the use of PHI for treatment, payment, and healthcare operations (TPO) as well as the minimum necessary use and disclosure of information. It also applies to the creation of a limited data set or de-identified information and formulation of standards for dealing with business associates (BA), mainly with contracts, application to information about the deceased, adherence to privacy practices and regulations, and application of covered entities' and constituents who are not covered entities (CEs), such as BAs. Any organization or person working in association with or providing services to a CE that handles or discloses PHI is a BA (Choi et al., 2006; McDavid, 2012; Peterson & Watzlaf, 2015; Wu, 2007). The HIPAA rule also requires a written authorization to collect, use, and disclose PHI for research purposes (Act, 2010).

The HIPAA security rule primarily addresses ePHI. It is designed to protect confidentiality, unauthorized use or access, threats to security, and integrity of PHI. There are different compliance

categories covered by the security rule (Annas, 2003; Choi et al., 2006; D. Solove, 2013). These are (Choi et al., 2006; HHS, 2013; Peterson & Watzlaf, 2015):

- Administrative safeguards - strict practices to manage security and personnel.
- Physical safeguards - physical protection of computers and the entire IT infrastructure and the buildings in which they reside.
- Technical safeguards - the use of technology to secure data in transit and to control and monitor access to information.
- Organizational requirements - BA contracts.
- Policies, procedures, and documentation requirements - this includes rules to protect individual PHI by defining how, when, and the specific reasons and conditions under which PHI can be disclosed.

HIPAA is a very complex law and could be costly and frustrating to clinicians, patients, and all major players in healthcare (Annas, 2003). One thorny issue when using telehealth technologies is exactly who is to be considered a BA, and how healthcare providers can get some of these businesses to enter into a business associate agreement (BAA) with them (Peterson & Watzlaf, 2015; V. J. Watzlaf, Moeini, Matusow, & Firouzan, 2011). For example, how do healthcare providers and other institutions who use Skype to provide health services to people from a distance convince the company that owns Skype, in this case, Microsoft, to engage in a BAA with them? HIPAA also mandates CEs to constantly monitor and perform routine auditing of their IT infrastructure. The audit reports are then used to find existing or potential violations to P&S (C. Wang, Wang, Ren, & Lou, 2010). Most hospitals and other health service providers contract with third party associates to perform the audits for them. Many individuals are of the view that using third party companies for auditing can introduce potential vulnerabilities because these companies have unlimited access to PHI. Therefore, BAAs between the CE and a BA of the CE are required.

Also, data use agreements (DUAs) that specify uses of PHI may be needed when the CEs work with BAs for different purposes such as research, quality improvement, or patient safety.

The Americans with Disabilities Act (ADA) and HIPAA offer minimal protection against the use of genetic data. The Genetic Information Nondiscrimination Act (GINA) was passed in May 21, 2008. This provides safeguards to prevent health insurance companies and employers from using people's genetic data to discriminate against them. For instance, the law prohibits an insurance company from using genetic information to set rates or premiums (Erwin, 2008; Hudson, Holohan, & Collins, 2008). Noncompliance with GINA could result in a fine of $300,000 per intentional incidence. For unintentional incidences, the fine could range between $2,500 and $500,000. GINA also provides an extension of the HIPAA confidentiality law to the use or disclosure of genetic information (Erwin, 2008; Hudson et al., 2008). Hence, securing genetic data should also be incorporated into P&S policies that govern health information.

The HITECH Act was passed by Congress in 2009 as part of the American Recovery and Reinvestment Act (ARRA). This was an extension of HIPAA which addressed P&S issues related to the use of technology, such as IT in healthcare. HITECH strengthened HIPAA enforcement, accumulating $14,883,345 in fines and penalties for violations (Act, 2010; D. Solove, 2013). Penalties have been as high as $1.5 million in certain instances. The new law also granted more powers to the OCR to enforce HIPAA. The HITECH Act increased penalties for HIPAA violations drastically from $100 per violation and capped at $25,000 per annum to $1.5 million annually. The tiered penalties are shown in Table 3 below:

Table 3: Breach Civil Monetary Penalties

Tier	Penalty Ratings
1.Reasonable Diligence (Did not know)	$100-50,000 for each violation; maximum of $1.5 million for the same violations in the same calendar year
2. Reasonable Cause (Should have known)	$1,000-$50,000 for each violation; maximum of $1.5 million for identical violations
3. Willful Neglect (Corrected)	$10,000-$50,000 for each violation; maximum of $1.5 million for identical violations in the same calendar year
4. Willful Neglect	$50,000 or more for each violation; maximum of $1.5 million for identical violations in the same calendar year

Data from (D. Solove, 2013) as well as information on the DHHS website show evidence of increased oversight and fines for HIPAA and HITECH violations, as shown in Table 4 below. Aside from the fines, there is also public shaming of the corporations whose information is displayed on the website.

Table 4: Example of Breaches and Fines

Breach Cause	Breach Summary
Not following risk management rules	Fresenius Medical Care North America (FMCNA) paid a fine of $3.5 million for failing to follow HIPAA's risk management rules.
Impermissible disclosure of ePHI	CardioNet has agreed to settle potential noncompliance with the HIPAA Privacy and Security Rules by paying $2.5 million and implementing a corrective action plan in 2017

Table 4 (continued)

Insufficient ePHI Access Controls	Memorial Healthcare System paid $5.5 million in 2017 for failing to have sufficient access controls to peoples ePHI
Theft of USB drive	Alaska Department of Health and Social Services settled with the Department of Health and Human Services (DHHS) in the amount of $1.5 million for violations in 2012.
Hard Drive theft	Blue Cross Blue Shield of Tennessee paid a fine of $1.5 million for an incidence involving unencrypted hard drives that were stolen from one of their facilities.
Data not erased from copier hard drives	DHHS fined Affinity Health Plan, Inc. $1,215,780 for mistakenly disclosing PHI of 344,579 people when it returned leased photo copiers without flashing the hard drives on the copiers.
Improper disposal of PHI	CVS Caremark fined $2.25 million for improper disposal of personal health information (PHI) in 2009 (labels from prescription bottles and old prescriptions).
In adequate HIPAA security safeguards and unauthorized access	Phoenix Cardiac Surgery paid $100,000 to DHHS for lack of HIPAA security safeguards and posting patient schedule on public Internet calendar-2012.
UN-Authorized use of PHI in training	Shasta Regional Medical Center was fined $275,000 for impermissible use of PHI to train its workforce in 2013.

As seen in Table 4, OCR is now imposing stiffer penalties on violators of HIPAA. Another significant change in HIPAA was the expansion of HITECH under the Omnibus rule, which was enacted in 2013 (Bendix, 2013). One significant part of the Omnibus rule involved the expansion of HIPAA to directly apply to BAs (D. Solove, 2013). About 20% of all violations were a result of violations by BAs (Act, 2010; D. Solove, 2013). In the past, CEs were required to enter into contracts with their BAs, but the CEs were held responsible for any violations by the BAs. However, under HITECH/Omnibus, BAs are now subject to direct enforcement and sanctions. This means BAs are held to the same high standards as CEs (Chaput, 2013; D. Solove, 2013; V. J. Watzlaf et al., 2011; Wu, 2007).

The Patient Protection and Affordable Care Act of 2010 (ACA) was signed into law by President Obama on March 23, 2010. It is said to be the most significant change in the health care system in the United States since Medicare and Medicaid (Huntington, Covington, Center, Covington, & Manchikanti, 2011). The law does not mandate businesses to provide health insurance to their employees. However, larger employers face penalties if they do not make affordable coverage available to their employees. Employers with 100 or more employees must comply by 2015 or face penalties. Employers with 50 or more had until 2016 to comply or face penalties. The law also requires all individuals to have health insurance. Failure by both business and individuals to obtain insurance can lead to potential fines. ACA prevents health insurance companies from refusing to insure people with pre-existing medical conditions. The incorporation of newer computer technologies in healthcare is bound to complicate things. Health service providers need to understand how to stay in compliance with healthcare regulations as they use these newer technology platforms.

3.3 ADVANTAGES OF INFORMATION TECHNOLOGY IN HEALTHCARE

The use of various forms of information technology (IT) for patient care has many advantages. Some of these benefits include improved access to information and decision support systems, cost savings, and overall efficiency/effectiveness in patient care (Bhuyan et al., 2017; Idowu, 2015; Kokkonen et al., 2013; Rindfleisch, 1997).

3.4 EXAMPLES OF ADOPTION OF NEW TECHNOLOGIES IN HEALTHCARE

According to the info-graphic page on HealthIT.gov, 8 out of 10 physicians surveyed reported that EHR use enhanced overall patient care (HealthIT.gov, 2013):

- 81% agreed that their EHR helped them to access patient information remotely.
- 64% said the use of their EHR alerted them to a potential medication error.
- 62% reported being alerted to a critical lab value.

With smartphones and other mobile devices set to overshadow PCs as the number one method of computing, both in the personal and professional environment, cyber criminals have turned their attention to mobile devices. A 2011 global study report released by Juniper Networks showed an increased rate of security threats to mobile devices, with Android-based devices showing a 400% increase in Android malware (Markelj & Bernik, 2012). It is therefore important to secure these platforms before using them in healthcare delivery in order to protect patient information (Gozalvez, 2011; Ifrim, Pintilie, Apostol, Dobre, & Pop, 2017; Kowitlawakul, Chan, Pulcini, & Wang, 2015).

A HIMMS survey conducted in 2011 captured interesting data related to the United States wireless-health market:

- Wireless-health saw an increase from $2.7M in 2007 to 9.6B in 2012.
- 80% or more of physicians owned smartphones and two-thirds accessed information on the web for professional needs
- 95% of physicians used their portable devices or smartphones to download apps for medical information (Gallagher, 2012)

Availability of mobile health apps is on the rise, spurred by an increase in demand (Burkhart, 2012; Gallagher, 2012) (see Table 5).

Table 5: HIMMS Survey results for number of mobile health apps in 2011

Application	Number of health applications available for download	Intended for consumer/ patient	Intended for healthcare professional	Number of downloads
iPhone	~6000	73%	30%	Unknown
Android	~600	81%	20%	3.5 million +
Blackberry	~200	70%	30%	Unknown

HIMMS survey conducted in 2011

Another survey conducted by HIMMS in December 2011 found that many more hospitals are allowing physicians to use mobile and wireless devices in their practice. Some of these devices are privately owned by the physicians. It is estimated that 25% of the 80 % of physicians who own smartphones and tablets utilize them in various forms of patient care (Burkhart, 2012). The survey also revealed that most institutions have acknowledged some P&S concerns, yet they have no P&S policies in place for the use of such devices (Gallagher, 2012). Although 41% of healthcare institutions allow doctors to use their personal devices, 28% of these devices retain PHI and 77% of doctors access data on public networks with those devices (Gallagher, 2012). This could lead to various P&S breaches as well as breaches of HIPAA, HITECH, and other healthcare regulations.

Research has further shown that there are no clear federal regulations for the use of mobile technology in healthcare (Giunti, Giunta, Guisado-Fernandez, Bender, & Fernandez-Luque, 2018;

Petersen & DeMuro, 2015). Until recently, the mobile market was mainly self-regulated. This is due in large part to the very nature of the technology. An example is a situation where a woman was reported to have used a commercial smartphone app as a "standby stethoscope" to monitor her infant daughter's heart condition. US Food and Drug Administration (FDA) approval was not needed for the device because it was supposed to be used for gathering "bio-feedback data" rather than for diagnosis (Burkhart, 2012). Congress in July 2012 finally signed into law the FDA Safety and Innovation Act to try to regulate mobile medical apps. This led to the establishment of a commission charged with finding ways to regulate mobile medical apps and reporting back to Congress within 18 months (Burkhart, 2012; Steinbrook & Sharfstein, 2012).

The FDA issued a final guidance on mobile medical apps on September 25, 2013, which first defined a medical app. According to the FDA, a mobile medical app is a software that runs on a mobile platform which is either used as an accessory to a regulated medical device or transforms a mobile platform into a regulated device (Kamerow, 2013). Most health-related apps are not regulated, as they are considered non-devices by the FDA definition of mobile apps. Examples are electronic versions of medical books and reference materials, educational apps for patients, or clinicians, general office apps, Generic tools (magnifiers, recorders and communication aids)(Giunti et al., 2018; Kamerow, 2013).

The FDA will employ "enforcement discretion" and will not regulate mobile medical apps that are not considered devices but can be used for diagnoses, treatment or prevention of diseases so long they pose a low risk to the public. Most disease tracking apps such as apps for diabetes, motivational or educational apps for dieting and exercising, smoked cessation, and other behavioral changes fall under this category(Kamerow, 2013).

The FDA will regulate apps that use attachments of any sort of gadget to a phone to measure, diagnose, or treat a medical problem, hence turning the phone into a controller or screen for the device. Any app that has the capability of turning the phone itself into a device such as using the phone's speaker phone for audiometry, or allows phones to be used for remote monitoring will be regulated under the same rule that the FDA applies to other devices (Kamerow, 2013).

Another technology that is being widely adopted in providing health services is Voice/Video over Internet Protocol (VoIP) technology. The problem with this widespread adoption is that regulatory agencies now have to play catch-up in order to regulate the industry (V. J. Watzlaf et al., 2011). There are many issues pertaining to HIPAA, HITECH, and other regulatory compliance with the use of VoIP for various forms of patient care (V. R. Watzlaf & Ondich, 2012). All mobile health technologies, including VoIP, use TCP/IP protocols and run on networks including the Internet. This renders them susceptible to all of the P&S vulnerabilities associated with such networks (Peterson & Watzlaf, 2015; V. J. Watzlaf et al., 2011). According to Watzlaf et al. (2011), there are no clear-cut guidelines for P&S and HIPAA compliance for the use of different consumer-based VoIP technologies in healthcare. This is also true for the use of other existing and emerging technologies such as social media, cloud-based computing, mobile technologies (e.g., smartphones, tablets, and apps), and multi-user health kiosks in providing care to patients.

The first step in securing PHI in these emerging systems is to develop a detailed understanding of the unique vulnerabilities associated with the use of such devices and technologies. Another issue involves determining whether third party vendors, such as those

providing consumer-based technologies like Skype and others, are considered BAs when used for tele-practice, and whether they fall under HIPAA, HITECH, and other regulations.

Information security should be the cornerstone of any HIPAA/HITECH and other regulatory compliance. It is reasonable to think that, in this information age, there cannot be HIPAA, HITECH, and state and federal compliance without procedures in place to safeguard patient information. A good P&S guideline must therefore reference the technical safeguard section of the HIPAA P&S standards for addressing access control, audit control, integrity, person or entity authentication, and transmission security to ensure HIPAA compliance (Maji et al., 2008; Peterson & Watzlaf, 2015).

4.0 INFORMATION SECURITY

Information security has been defined as the task of safeguarding information that is digital in nature. A successful information security system should have multiple layers of security by employing the following procedures to protect computer systems and information (Bendix, 2013; Merkow & Breithaupt, 2014; B. Smith, 2008; Whitman & Mattord, 2010).

Physical security should be used to offer protection for physical items, objects, and sensitive areas from unauthorized access to misuse. This is normally accomplished by controlling access to sensitive rooms or areas in the organization, access to network cables and devices, and hardware and data disposal procedures.

Workers and other authorized individuals who have access to an institution's computer devices and data should be protected. This can be accomplished by instituting proper personnel security procedures such as employing security guards and protecting personnel identity in some cases.

Logical security must be well designed to protect computer infrastructure, data, and information through a string of encryption procedures, secured accounts and passwords.

Effective operations security should be put in place for the protection of an organization's operations or activities through adoption of secured operational procedures such as allowing employees to use only licensed software and using computer systems only for business activities. This will lower the risk of downloading malicious software that could introduce vulnerabilities into the computer devices like kiosk computer systems, software and a kiosk itself.

Communications security is very important in the protection of the medium of communication, technology, and the content of communication. This may be in the form of data encryption and using secure means of communications or secure data transfer protocols. Such security measures are even more critical for devices such as a multi-user health kiosk that stores and transmits large amounts of PHI in electronic format.

Careful attention must be paid to implement effective network security to offer protection for computer network components, connections, and data, through appropriate procedures to address access control, firewalls, intrusion detection and prevention systems, system redundancy, change management, and single point of failure. Effective network security has become even more important since all computer systems and technologies, including kiosks, are networked.

Servers and PCs must be protected through adoption of measures and procedures to manage software licenses, patches (operating system and other security updates), and laptop security. Keeping up with software and computer updates helps to lower privacy and security vulnerabilities.

An important factor that is often overlooked is IT security policies, procedures and practices. Development and implementation of security, privacy, acceptable use, and backup (BC)/disaster recovery (DR) planning and policies can offer tremendous protection to computer devices and information/data.

Up-to-date anti-virus (AV), anti-Spyware and SPAM filters should be deployed to protect against various vulnerabilities such as downloading malicious programs, hackers, and spammers, to minimize the possibility of a security or privacy breach. This is necessary to prevent

unauthorized access to users' personal data, destruction of computer infrastructure and/or disruption of normal operation of the computer system or an entire organization.

Attention must also be paid to software security to offer protection through identification of bugs and mission-critical apps, changes and updates, and testing. Bugs and incomplete updates can introduce security and privacy loopholes that can be exploited to gain access to user data or information.

Having a good understanding of information security allows us to protect information that has value. Information security must therefore be shaped to protect the characteristics of information including confidentiality, integrity, availability, privacy and non-repudiation:

Confidentiality strives to assure that only authorized users can view the information (Buckovich, Rippen, & Rozen, 1999; S. Das & Mukhopadhyay, 2011; Russell & Gangemi, 1991).

Integrity helps to make sure that information is accurate and that no authorized or unauthorized person or malicious software has falsely or illegally altered the information (S. Das & Mukhopadhyay, 2011; Merkow & Breithaupt, 2014; Russell & Gangemi, 1991).

Availability allows systems administrators to take steps to assure access to computer systems and data/information by authorized users when needed and in a timely manner (Ciampa, 2008; S. Das & Mukhopadhyay, 2011). This is very important, especially in computer systems that are used to provide health services to people. HIPAA and HITECH rules require systems to be reliable and highly available for patient care(HHS, 2013).

Privacy accords users the ability to keep their personal information secret from others. Breach of confidentiality constitutes a breach of privacy (Buckovich et al., 1999; D. G. O'Brien & Yasnoff, 1999). Appropriate measures must be put in place to protect privacy of users as they

patronize the different health applications and technologies that are being developed. Violations could result in stiff monetary and other penalties (HHS, 2013; D. Solove, 2013).

Non-repudiation allows us to verify the origin of a message. It ensures that the origin of the message is legitimate. This helps to prevent impersonation on computer networks (Djenouri, Khelladi, & Badache, 2005; Merkow & Breithaupt, 2014). It also prevents malicious people from employing different tricks such as phishing and man-in-the middle attacks to gain access to system resources including users' data/information.

It is prudent to envision information security beyond just protecting information. Because information is stored on computer hardware, manipulated by software, and transferred by various means of communication, all these areas must be protected. Information security in healthcare must be performed within the framework of HIPAA/HITECH. Sections of HIPAA address medical privacy and confidentiality. Healthcare providers, under this act, are required to abide by the electronic health information standards put in place by Congress (D. G. O'Brien & Yasnoff, 1999; Peterson & Watzlaf, 2015).

4.1 DEFINITION OF INFORMATION SECURITY

Healthcare providers and their associates as well as healthcare technology developers must understand that information security has moved from "just good business practice" to a legal requirement. They are obliged by various laws to protect privacy and confidentiality, provide security, and disclose data breaches (Gaff, Smedinghoff, & Sor, 2012; Peterson & Watzlaf, 2015).

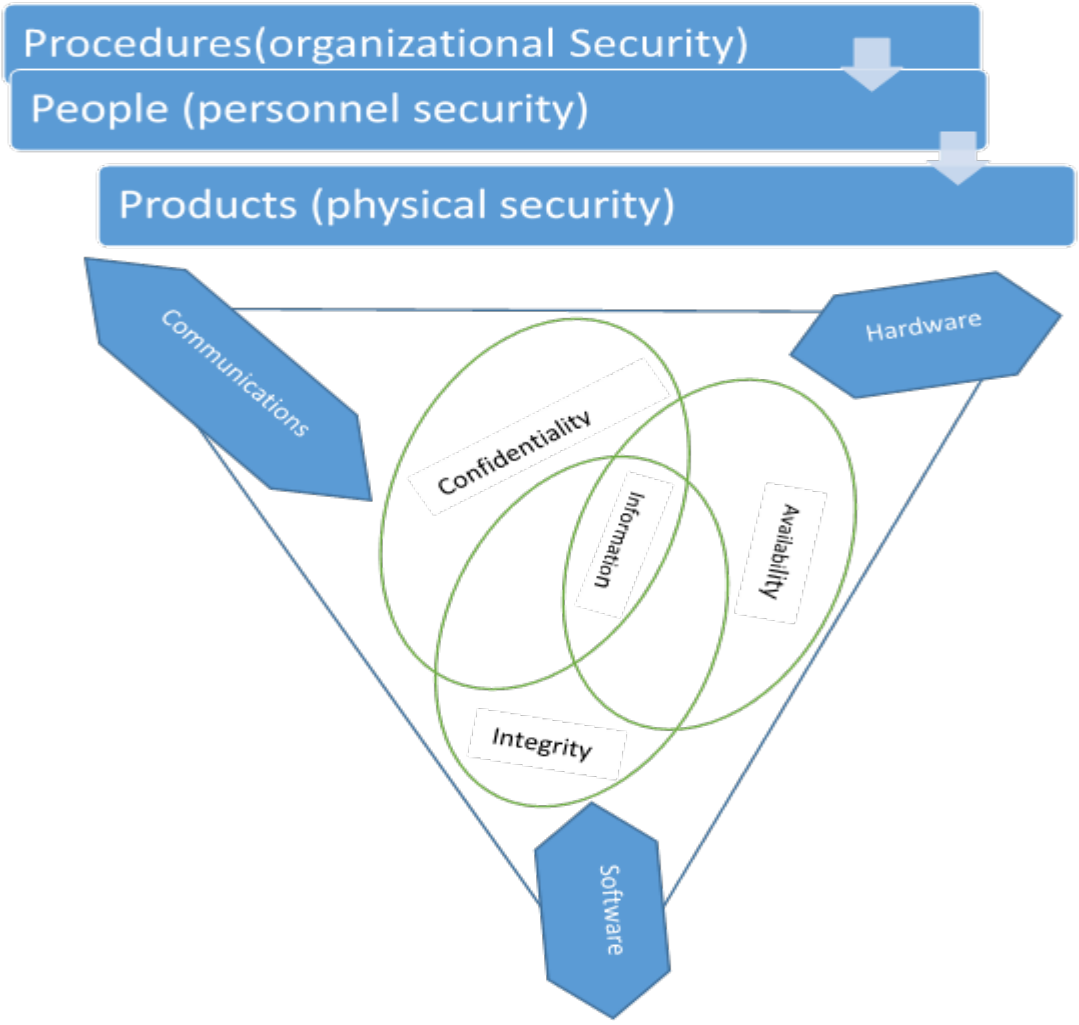

Figure 1: Information Security Components

Security measures can be very complex to implement. As illustrated in Figure 1, information, hardware, software, and communication should be protected in three layers: products, people, and procedures. These three layers work together to achieve the best results. *Products* refers to the physical security around the data. This could be door locks, intrusion detection systems, or computer firewalls. *People* refers to people who use the systems to perform various activities. *Procedures* are rules, plans, and policies that have been put in place by organizations to

guard against improper use of products, information, and data (Ciampa, 2008; Merkow & Breithaupt, 2014; Wu, 2007).

A more complete definition of information security is, therefore, *"that which protects the integrity, confidentiality, and availability of information on the devices that store, manipulate, and transmit the information through products, people and procedures (Ciampa, 2008)"*.

4.2 CHALLENGES OF SECURING INFORMATION

Securing networks and applications, computer devices, especially mobile devices, web-based applications and kiosk systems is a daunting task in today's information age (Conti et al., 2018).

Speed of attacks makes it difficult for IT professionals to detect and stop or prevent attacks from being orchestrated. Attackers have access to very sophisticated tools that enable them to scan and exploit weaknesses and launch attacks on computer systems with extraordinary speed (Turban, King, Lee, Liang, & Turban, 2015). For example, the Slammer worm infected 75,000 computers in the first 11 minutes after its release in 2003, causing massive disruption of service. The worm scanned 55 million computers per second to find vulnerabilities that could be exploited to gain unauthorized access to computer systems and information (Ciampa, 2008; Householder, Houle, & Dougherty, 2002; Kizza, 2013b; L. Zhang & Zhao, 2008).

Sophistication of attacks is a huge problem in information security. Attackers make it difficult for IT personnel to distinguish attacks from legitimate network traffic. This is because attackers employ common Internet tools and protocols in their attacks (e.g., Telnet, ping, Port Scanners, SQL injection, and malicious applications (Householder et al., 2002; Sanatinia &

Noubir, 2015; Turban et al., 2015). The simplicity of attack tools has also made it easy for people with little or no computer skills or technical skills to infiltrate computer systems and applications to gain access to sensitive information or disrupt entire computer systems or networks. Most of these tools are readily available on the internet. Some come with step by step instructions on how to use them (Ciampa, 2008; Householder et al., 2002; Kizza, 2013b; Merkow & Breithaupt, 2014).

There has been a surge in "Zero Day" attacks. The simplicity and easy availability of attack tools have made it easy for hackers to discover new vulnerabilities and launch attacks with little or no warning. IT security experts are left fighting against time to find fixes (Householder et al., 2002; Kizza, 2013b; Russell & Gangemi, 1991).

Delays in patching hardware and software products can lead to serious consequences such as fines loss of information/data and disruption in services. With the increase in attacks, software and hardware vendors are constantly fighting against time to patch their systems against security vulnerabilities. System administrators also have to make sure their systems are updated with the latest patches. This can turn out to be a daunting task as new vulnerabilities are discovered every year or, in some cases, every day (Householder et al., 2002; Kizza, 2013b).

The distributed nature of attacks makes it difficult to determine the source of an attack. Most attacks are launched from multiple (thousands) of computers, mostly against a single computer, making it almost impossible to prevent an attack by blocking a sole source. This very popular technique is employed by attackers to launch denial-of-service (DoS) attacks (Sumra, Hasbullah, & AbManan, 2015), which can result in violations of HIPAA and HITECH as well as penalties and fines (D. Solove, 2013).

User confusion is a major problem in this highly mobile, web-oriented and self-service (kiosks) environment. Users are increasingly being asked to make security decisions on their

systems with little or no guidance. For example, a user with little or no knowledge of information security may be asked questions such as "Is it okay to open this port?"; "Is it safe to quarantine this attachment?"; or "Do you want to include the installation of an add-in?" (Ciampa, 2008; Kizza, 2013b). This is a huge problem as users, by granting these privileges to these apps, can mistakenly provide access to their sensitive information. Attackers and hackers can then escalate those privileges to gain access to entire computer systems or networks, resulting in very serious HIPAA and HITECH security and privacy violations(Act, 2010; D. Solove, 2013).

Disgruntled employees and insider attacks are a major source of attack against computer systems (Merkow & Breithaupt, 2014; G. S. Smith & Futter, 2015). For example, an attack was perpetrated by a former employee of a subcontracting company who was working on computer systems for the Maroochy Shire Council's sewage system in Australia in the year 2000. After the employee was fired by the subcontracting firm, he used various means to undermine the computer system controlling the waste management plant, causing millions of liters of raw sewage to spill into local parks. The employee then tried to get the water and sewage company to hire him to resolve the problem (Cardenas et al., 2009).

4.3 POSSIBLE INFORMATION/ NETWORK VULNERABILITIES OR ATTACKS

Vulnerabilities are weaknesses in data networks, devices, and software that make them targets for attacks. The best way to make data networks, devices, and software secure is to identify, understand, and mitigate the mode of attack posed by possible vulnerabilities (D'ESTE & Taylor, 2003; Kizza, 2013a; Merkow & Breithaupt, 2014; Ritchey & Ammann, 2000).

4.4 MEDIA-BASED VULNERABILITIES

These are vulnerabilities based on the network transport media. Network administrators use various tools to help them to monitor network traffic to trouble-shoot problems as well as to perform different administrative functions on the network. These same tools can be used by an attacker for malicious reasons (Ciampa, 2008; Kizza, 2013a; Orebaugh, Ramirez, & Beale, 2006; Paliwal, Mudgal, & Taterh, 2015). One example of media-based vulnerabilities is the protocol analyzer, which captures packets of information or data in order to decode and analyze their contents (Ballmann, 2015). Port Mirroring is utilized for monitoring network traffic by copying each data packet from one network switch port to another. For example, a network administrator can attach a computer to a switch on a network that supports port mirroring to monitor network traffic. Network tap (test access point) allows a computer device to be installed by a network administrator between a switch, router, or firewall to monitor traffic (Ballmann, 2015; Orebaugh et al., 2006). This is usually for testing purposes. A hacker can exploit the network tap to gain access to the underlying computer network, resulting in a breach of HIPAA and HITECH privacy and security rules (HHS, 2013).

The best way to limit media-based vulnerabilities is to have a good inventory of all network devices and their functions on the network. The network administrator should run periodic scans to detect any unauthorized devices (e.g., network dongles, malicious switches, and computers) that are attached to the network. Another way is to prevent access to false ceilings and to make sure that all access points are secured and that no network wires are exposed. All network ports that are not in use, especially in vacant buildings or unused work areas, should be disabled (Ballmann, 2015; Merkow & Breithaupt, 2014).

Administrators should also protect their networks from network sniffers (Awad, 2015; Ballmann, 2015; Orebaugh et al., 2006) in a variety of ways:

- Host-to-host VPN encryption should be employed to hide the data within the packets from sniffers. If the right techniques are employed, this protection approach could even be used to hide information about the ports and communication protocols used.
- Data packets can also be protected by employing application-level encryption such as the Secure Socket Layer (SSL).
- Deploying switches on a network instead of hubs makes the network more difficult to sniff.

Good detection techniques also help to identify the presence of sniffers on a network (Ballmann, 2015):

- Interfaces operating in promiscuous mode are a sign of sniffers' presence.
- Sniffers may also exhibit characteristics like superfluous DNS lookups, network latency, driver issues, and suspicious application behavior.
- Strong organizational policies can provide an effective safeguard against different sniffing tools. For example, the University of Pittsburgh Computer Services department does not allow individuals to install their own switches, hubs, or routers on the university's computer network.

4.5 NETWORK DEVICE VULNERABILITIES

Attackers can also exploit vulnerabilities in the network devices themselves. This is accomplished by taking advantage of weak passwords, malware, default accounts, backdoors, and privilege escalation (Ballmann, 2015; Merkow & Breithaupt, 2014). Using weak passwords makes it easy for others to guess the passwords. However, the problem with stronger or complex passwords is that they are very difficult to memorize. Nonetheless, users must be encouraged to create stronger passwords devoid of personal information like favorite pets, cars, and nicknames (Merkow & Breithaupt, 2014). This will help to prevent occurrences of clandestine activities such as privilege escalation to gain unauthorized access information, data and other system resources.

Malware is shorthand for "malicious software." Malware includes viruses, spyware, and other types of harmful software designed to disrupt operations, gather information without user permission or knowledge, gain unauthorized access to systems resources, and instigate other potentially abusive or damaging behavior (Ballmann, 2015; Ciampa, 2008; Kizza, 2013a). Systems must be protected against malware through installation of good antivirus, anti-spyware, and anti-adware programs. Administrators must take steps to download and install updates and patches for their systems. Users must be educated about potential activities (e.g., visiting suspicious internet sites, not updating their antivirus software, not opening suspicious email messages and attachments) that could expose their systems to viruses. Malwares can cause system failure, stealing and or loss of data/information. Systems like health kiosks are at greater risk because they are constantly connected to the internet.

Default accounts are created automatically by a device or device manufacturer instead of a network administrator. These types of accounts are supposed to be used for initial device setup,

and they have full administrator privileges. Default accounts are supposed to be deleted or disabled after initial installation, but they are not deleted most of the time. Attackers will usually exploit these default accounts first, then create administrator accounts for themselves once they gain initial access to the system. This provides them with unlimited access to the network/system to perform malicious administrative functions. Disabling or deleting default accounts should be clearly stated in organizations' information security policies (Ballmann, 2015; Schwingenschlögl & Pilz, 2001).

Backdoors are usually used by programmers and system developers for testing during software/system development. They provide "emergency" access to system and software components in the event of a malfunction. Backdoors can be exploited by adversaries, however, to gain unauthorized access to computer systems. Telnet is the protocol of choice for such mechanisms. Backdoors are normally accounts, devices, and software set up without the knowledge of an administrator, and they are not easily detected (Neumann, 2015). Attackers can therefore use backdoors to gain access to various information and other devices on the network (Yin Zhang & Paxson, 2000). If backdoors are not uncovered and managed properly, cyber criminals can exploit them, leading to HIPAA and HITECH P&S breaches with dire consequences (Sametinger, Rozenblit, Lysecky, & Ott, 2015).

Privilege escalation is a major concern in client/server environments where devices and applications have become ever more interconnected. Operating systems, applications/software, and network devices can be at risk of privilege escalation, which entails users giving themselves greater permission than they are supposed to have (Ciampa, 2008; Provos, Friedl, & Honeyman, 2003). This can lead to serious HIPAA/HITECH violations in healthcare systems when unauthorized workers gain access to users' PHI and other information. Privilege escalation can be minimized by periodic IT audits to make sure that users/workers do not have access to resources

they are not allowed to have. Another method is privilege separation, which segments network resources into privileged and unprivileged sections, enabling assignment of different levels of privilege to resources and network devices (Provos et al., 2003). There should also be strict policy enforcement against privilege escalation (Bugiel et al., 2012).

Denial of Service (DoS) can affect system availability. This is a very major concern in health applications for which non-availability of a system can jeopardize people's health outcomes (Sametinger et al., 2015). This network attack vulnerability involves an attacker using various methods to consume all resources on a network so that legitimate devices or users are not able to connect (Awad, 2015). This can result in interruption of service. In this type of attack, the attacker uses a computer device or program to make repeated requests to a server but never responds. More requests are sent to the server and eventually the server gets overwhelmed as it waits for a response from the attacker's computer, making it unable to respond to legitimate requests (Awad, 2015). This violates the aspect of HIPAA which mandates that information is to be available at all times (Djenouri et al., 2005; Householder et al., 2002). One of the best ways to reduce the impact of DoS attacks is for organizations to replicate their servers at backup centers (Awad, 2015; Singhal, Winograd, & Scarfone, 2007). DoS attacks can also be prevented by media access control (MAC) address filtering. This technique usually uses a network edge device to filter MAC addresses and internet protocol (IP) addresses from computers requesting information. If the MAC address and the IP address filtered do not correspond with the network lease information stored in a special database on the organizations network, then any request from that MAC address and the IP address is dropped (Caves, Altarac, & Ilgun, 2008; Kassi-Lahlou, Mansour, & Michel, 2014).

An attacker can also exploit vulnerabilities in communication protocols as well as weak encryption procedures to launch Man in the Middle attacks. This allows the attacker to intercept

information in a data packet before it gets to the recipient. The attacker can either modify the information or fabricate additional information before it reaches the recipient. The adversary can also use this technique to gain unauthorized access to PHI and other sensitive information in transit (S. Das & Mukhopadhyay, 2011; Srivastava, Awasthi, Kaul, & Mittal, 2015). This type of attack can be minimized by implementing cryptography in systems such as a health kiosk. If data packets are encrypted, they are almost impossible for the "man-in-the-middle" to read information contained in the packets (Awad, 2015; Ciampa, 2008; S. Das & Mukhopadhyay, 2011; Householder et al., 2002).

5.0 SECURITY VULNERABILITIES OF EMERGING TECHNOLOGIES IN HEALTHCARE

Emerging computer technologies being adopted in healthcare and other health services offer tremendous advantages. However, they are vulnerable to serious security threats if the right steps are not taken to secure them before adoption and use in healthcare and delivery of other health services.

5.1 WIRELESS NETWORK SECURITY CONCERNS

Wireless security concerns are on the rise in the realm of PHI due to the increased use of mobile devices by healthcare providers (Martínez-Pérez, De La Torre-Díez, & López-Coronado, 2015). A recent Manhattan Research survey found that about 30% of physicians own iPads (Kate & Borten, 2010). The survey showed that some of the physicians have used such devices to access, view, and store PHI on their mobile devices (Kate & Borten, 2010). This poses an increase in P&S threats to information, including PHI. Seventy-three percent of physicians from a recent survey said they text other physicians about work. Thus, keeping the information exchanges secured is a major concern (Harman et al., 2012).

Securing mobile devices including mobile applications is a daunting task for IT professionals. This stems from the fact that mobile devices and the apps that run on them are largely designed for individual use and not for centralized management (Harman et al., 2012; Martínez-Pérez et al., 2015). 802.11 is a suite of protocols mainly used to protect wireless networks

and devices. Wireless devices and access points, like other network devices, are vulnerable when configured based on default administrative configurations (accounts and passwords). These configurations are commonly known to anyone who owns a similar device or has access to the documentation or manuals of such devices (Ballmann, 2015; networks, 2009). Another source of vulnerability is a wireless access point that uses a wireless adapter predisposed to remote exploit attacks (Ma & Wang, 2015; networks, 2009). A type of vulnerability that is usually overlooked is device loss or theft. Many users do not have passwords on their mobile devices. People usually do not encrypt the data on their devices either. Therefore, if these devices are lost or stolen, the information on the devices (including PHI if stored on such devices) may end up in the wrong hands (Peterson & Watzlaf, 2015). This problem is even more acute when these devices are used to deliver any form of health service to people that involves the handling of PHI in any form.

Most wireless devices and networks are secured by means of access control. This is usually done by limiting device access to the access point (AP). Restricting access to the AP means that only authorized devices are permitted to connect to the access point and become part of the network. Since the access point is responsible for connecting and transmitting data to all devices on the wireless network, protection of devices on the network should start with securing the access point (Awad, 2015; Ciampa, 2008; networks, 2009). Encryption is then used to secure the data and information transmitted between the devices on the network.

Media access control (MAC) address filtering is utilized to limit access to access points. This is done because every wireless device has a MAC address that uniquely identifies it. This is sometimes confused with user access restriction, which involves restriction placed on what authenticated users may do once they gain access to the network. MAC address filtering is used to

prevent certain devices from accessing a wireless network (Celebi, Joseph, Bilange, Marx, & Conroy, 2015; Ciampa, 2008; Kizza, 2013b).

Although MAC address filtering provides some level of protection, vulnerability is present because MAC addresses are initially exchanged in an unencrypted manner. Hence, an attacker can intercept and use the MAC address of an approved device to gain access to the network. Managing a large number of MAC addresses can be quite difficult for an IT department due to the large number of computing devices present on an organizations' network. It also does not make it easy to allow guest users on the organization's network.

Wired Equivalent Privacy (WEP) keys are considered a better alternative to MAC address filtering, as they provide encryption to data/information exchanged on a wireless network. WEP keys provide P&S equivalent to wired networks. WEP requires a 64-bit or 128-bit encryption key with an initialization vector of 24 bits. This short initialization vector makes it is easy for an attacker to decipher the key (Awad, 2015; Paliwal et al., 2015).

Wi-Fi Protected Access (WPA) was designed to be used for both authentication and encryption. It was made up of a PreShared Key (PSK) for authentication and a Temporal Key Integrity Protocol (TKIP) for encryption. PSK uses a passphrase as the encryption key. This phrase is created and entered into the access point and then pre-entered into all devices before they can join the network. Hence, PSK is used for both authentication and encryption (Reddy & Lakshmi, 2014).

TKIP has replaced WEP as an encryption technology and has some advantages over WEP, which uses a static 40-bit key for encryption, while TKIP uses a 128-bit key. This generates 280 trillion possible keys for a given data packet. This level of randomness makes TKIP a better encryption algorithm than WEP (Ciampa, 2008; networks, 2009; Paliwal et al., 2015). TKIP also

replaces WEP's Cyclic Redundancy Check (CRC) with Message Integrity Check (MIC) to prevent an attacker from capturing, altering, and resending data packets. TKIP can be combined with other technologies (like biometric authentication) to achieve even greater protection.

5.2 SECURITY RISKS POSED BY MOBILE DEVICES

The proliferation of mobile devices has increased the P&S concerns of most IT P&S experts. The healthcare industry has also seen its share of this massive shift to mobile computing (Kelley, Cranor, & Sadeh, 2013; Potter, 2007). A recent survey demonstrates that there were more than 165,000 mHealth applications in the world as of 2015. This number is supposed to double every year, with projections showing that there will be 1.7 billion mHealth users worldwide by the end of 2018 (Mabo, Swar, & Aghili, 2018). Mobile solutions have the main advantage of eliminating the need for wires and thus reducing clutter. They also offer convenience, workflow improvement, real-time voice access, and immediate and easy communication with people and machinery(Mabo et al., 2018). Despite all these advantages, mobile devices pose huge P&S risks (Abbott, 2010; Agarwal & Sebastian, 2014). Aside from having all the security risks of wireless communication networks, mobile devices pose other P&S risks because they are small and can easily be lost or stolen (Abbott, 2010). Today's mobile devices have quite substantial storage and the capacity to connect to both cellular and local Ethernet networks including personal area networks like Bluetooth. This renders them susceptible to both global and local attacks (Potter, 2007).

The use of mobile devices in healthcare amplifies these P&S concerns due to the sheer nature of the healthcare industry. Most organizations that provide health services have weak, or in

some cases missing, policies for the use of mobile devices. They typically lack procedures for workforce training and monitoring in place to protect people's privacy (Kate & Borten, 2010). Mobile P&S risks can be categorized in three main areas:

- Breach of data when at rest on a mobile device
- Breach of data occurring during transmission of data to or from the mobile device
- Breach of data occurring during transmission from the mobile device into the organization's network

There are multiple means by which a breach to mobile devices can occur. Some of these breach channels include:

Mobile Malware: The increase in the number of people using mobile devices has led to an increase in criminals writing malware applications that target mobile devices. Some of these criminals are coming up with "malware for profit," or they simply cause disruptions in mobile services. Most of these malwares come in the form of legitimate mobile apps injected with malicious code (Kate & Borten, 2010; Kelley et al., 2013; Markelj & Bernik, 2012; Martínez-Pérez et al., 2015). These apps then compromise the mobile device to steal sensitive information, gain access to other network resources, and launch even bigger attacks on other devices on the network (Kelley et al., 2013). A report from McAfee found six million malwares in the first quarter of 2011 alone. What makes the phenomenon more worrisome is that many of these rogue apps have infiltrated the app stores on mobile devices and made themselves available for download (Martínez-Pérez et al., 2015; Rose, 2011). McAfee has reported a new version of Zitmo mobile malware that was created to steal user information such as passwords and bank account numbers on some operating systems like the Windows Mobile system.

Lack of Visual Privacy: It is very difficult to prevent other people from viewing one's mobile screen, especially when it is used in an open area (T. Kwon & Hong, 2015). Due to their portability, mobile devices tend to be used by most people in the open. Hence, it is easy to expose confidential data/information (e.g., confidential PHI) to unauthorized persons in violation of HIPAA rules (Britton & Britton-Colonnese, 2017; Kate & Borten, 2010; Markelj & Bernik, 2012; Rose, 2011).

Consumerization of Devices: Mobile devices have become more powerful, less expensive and more easily available. Hence, most individuals including healthcare workers use their personal mobile devices such as smartphones for business (Kate & Borten, 2010; Kelley et al., 2013; Markelj & Bernik, 2012). According to HIMSS, P&S remain a major concern for the adoption and use of mobile technology in healthcare. Data from a HIMSS survey showed that 41% of providers allow their personnel to use their own mobile devices for work-related activities. The survey further demonstrated that "Bring your own device" (BYOD) policies pose major P&S challenges to IT professionals with responsibility for managing and protecting PHI on these devices. Among users with no protection, 28% had devices that retained PHI and 77% used their devices on public, unsecured networks (Gallagher, 2012). For example, an email message sent from such a device as a means of collaboration between physicians could be intercepted by an attacker and lead to a breach in confidentiality. Physicians surveyed have also acknowledged using devices provided by hospitals for personal reasons (Kate & Borten, 2010), which makes it even more difficult to secure such devices.

Varying Operating Systems: Various mobile devices run on different operating systems or software platforms. This lack of standardization in the number of operating systems used on mobile platforms makes it even more difficult to implement P&S procedures to protect devices, including

the data on these devices (Britton & Britton-Colonnese, 2017; Kate & Borten, 2010). Hospitals and healthcare providers should therefore endeavor to buy standard mobile platforms for employees to use for business purposes. Healthcare providers can also invest in third-party or commercially available technologies to help manage divergent mobile platforms used by their staff.

Vulnerable Connections: Users are still likely to use unsecured connections at times even if the healthcare unit provides them with a secured means of connection such as a Virtual Private Network (VPN). This usually occurs when using the devices for personal reasons (Kate & Borten, 2010; Patton et al., 2014).

Loss and Theft of a Device: This is a very serious issue. Of all the HIPAA P&S breaches posted on the U.S Department of Health and Human Services (DHHS) website since 2009, theft and loss of portable devices and media have accounted for the highest number of breaches. This issue is even more acute because most mobile devices are not secured. Unencrypted data stored on the devices could be exposed in the event that the device is lost or stolen (Britton & Britton-Colonnese, 2017; Kate & Borten, 2010; Rose, 2011).

Insiders, Human Error: Security experts believe that company insiders and human error pose one of the greatest threats to data, information, and network security(Bhuyan et al., 2017). Two hundred and sixteen respondents from a recent survey by Unisphere Research in 2011 said that human error and privilege escalation were major concerns for information security. Seventy-seven percent of the respondents were from financial institutions, and 56% were from non-financial institutions (Kizza, 2013a).

Lack of Awareness: A survey by McAfee and Carnegie Mellon University showed that one third of employees keep work-related and sensitive information on their mobile devices. Ninety-

five percent of them said they were unaware of company P&S policies, even though these companies had well-defined policies in place. Most of the companies acknowledged widespread employee ignorance on how security, permissions, and other access settings work(Bhuyan et al., 2017; Kizza, 2013b) .

Bluesnarfing: When the Bluetooth on a user's mobile device is enabled, rogue software or an individual can breach the connection to gain access to information on the device. This is a major issue when mobile users exchange information with other mobile users or transfer data between devices via Bluetooth. It turns out that many users are unaware of this loophole (Ciampa, 2008) (Bhuyan et al., 2017; Bindahman & Zakaria, 2011; Kizza, 2013a; Patton et al., 2014).

Eavesdropping: Most mobile networks, as well as mobile devices, operate in what is called promiscuous mode, in which a node on the network captures data packets intended for other nodes (Awad, 2015). This is done to improve efficiency on the network. Yet it poses a security threat when a routing protocol uses this mode to learn different routes on a network in order to effectively and efficiently transmit data across the network (i.e., in the form of malicious code or payload). This same feature can also be employed by a malicious individual or software to eavesdrop on data in transit. The only effective solution available is cryptography, which ensures confidentiality but does not eliminate the security threat (i.e., does not prevent people from eavesdropping) (Awad, 2015; Beretas, 2018; S. Das & Mukhopadhyay, 2011; Djenouri et al., 2005; Kelley et al., 2013).

5.3 PRIVACY AND SECURITY ISSUES OF WEB-BASED APPLICATIONS

The need to service more than one person at a time, the popularity of the Internet, and low development cost have led to the development of web-based applications. The healthcare arena is no exception, as more and more e-Health applications are being developed to meet patient needs (Bhuyan et al., 2017; Maji et al., 2008; Weinstein et al., 2014). Web-based applications are expected to have a market exceeding $1 trillion in a few years. There is already a host of P&S concerns with the use of web-based technologies and software.

To secure web-based/Internet-based applications and users, it is important to understand the architecture of web-based applications. Basically, web-based applications use three-tier architecture made up of Web clients, network servers, and databases to support different back-end information systems (Beretas, 2018; Ciampa, 2008; Joshi, Aref, Ghafoor, & Spafford, 2001; Kizza, 2013a). For commercial web-based systems such as e-commerce and mobile health, there are other middleware applications that function between the network servers and back-end systems for proper interoperability (see Figure 2) (Joshi et al., 2001; Linthicum, 1999). Middleware is computer software that provides services not available in operating systems, making it possible for diverse applications to interconnect, communicate, and perform different input output functions (Beretas, 2018; Linthicum, 1999). One example is the Java application developed by Sun Microsystems that was later purchased by Oracle, which allows inter-connectivity and interoperability between computer software and hardware. Hence, middleware is sometimes referred to as “software glue” (see Figure 2). All network security vulnerabilities such as inadequate authentication, weak passwords, lack of encryption, and malware are still present for

web-based applications (Ballmann, 2015). These complications in web-based applications make it even more difficult for IT administrators to protect such systems (Kizza, 2013a).

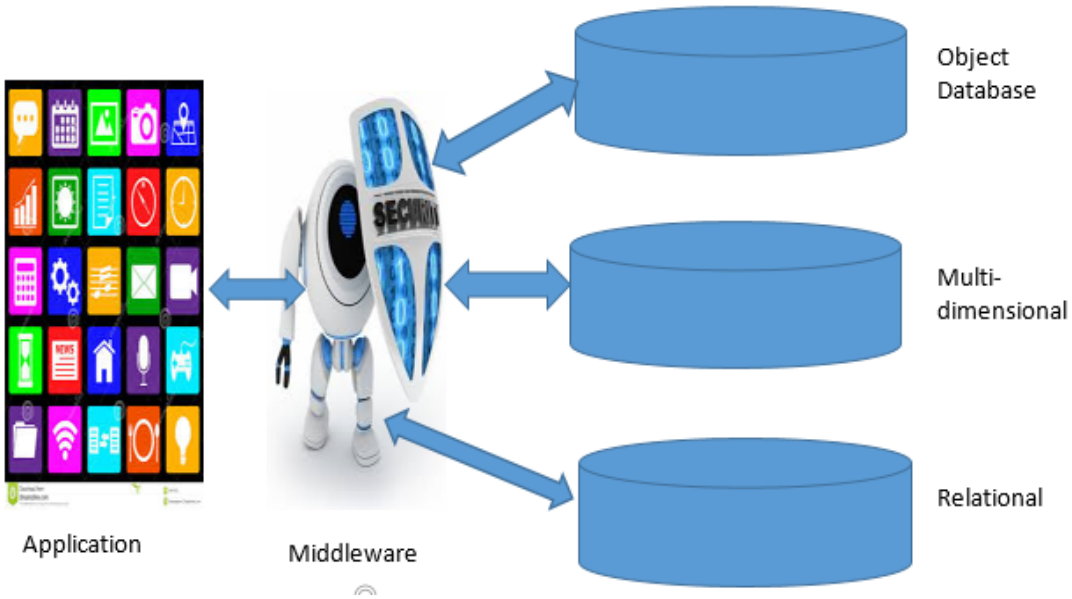

Figure 2: Architecture of Web-based Applications

Part of the process of protecting web-based applications requires protecting web browsers against attacks involving cookies, JavaScripts, Java, ActiveX, and cross-site scripting. Cookies are files containing information about various user online activities that are used to set user-specific preferences to better serve online content to users (Dadkhah, Beck, & Jazi, 2014; Sayed, Traore, & Abdelhalim, 2014). Cookies are usually stored on users' computers. Cookies by themselves do not pose security risks, as they do not contain specific user information like user names and passwords. They do, however, pose privacy risks, as they can be used to track users' online activities and prompt targeted presentation of online content such as advertisements and sometimes

unwanted content to users (Bouguettaya & Eltoweissy, 2003; Ciampa, 2008; Joshi et al., 2001; Kizza, 2013a; Lepofsky, 2014).

JavaScript was developed by Netscape to help websites run more smoothly and efficiently. For example, instead of loading large image files and other content each time a user visits a website, a button or link can be provided on the website for the user to click, which in turn would run the JavaScript to load an image or specific content to the user. However, the fact that the script can load an executable program to run on the website poses serious P&S issues. An attacker can inject its own code to download and execute a malicious program/application to steal personal information (Bouguettaya & Eltoweissy, 2003; Ciampa, 2008; Joshi et al., 2001; Sayed et al., 2014).

Java, unlike JavaScript, is a complete, object-oriented, programming language developed by Sun Microsystems. The advantage of Java is that it can be used to create small, stand-alone, machine-independent applications called applets. These can be used to add different functionalities and features to web pages. The applets are stored on the web server and downloaded along with other HTML code to users' computers to perform interactive animations, immediate calculations, and other simple tasks very quickly. Hackers or attackers can inject hostile Java applets onto websites to access data, passwords, and other information on both the user's local computer and the network server. The most widely-used defense against malicious Java applets has been sandboxing, which creates a security fence to keep Java applets away from private data and other areas of the local computer (Ciampa, 2008; Joshi et al., 2001; Lepofsky, 2014). However, this is not a complete solution, as sandboxes can sometimes break down. One way that users can protect themselves is to only run signed Java applets. Signed Java applets have information to prove that

the program is from a legitimate source, whereas unsigned ones are usually not from trusted sources and thus have no information about the source.

ActiveX is not a scripting program, but rather a set of rules developed by Microsoft to control how applications share information. ActiveX controls, also called add-ons or ActiveX applications, are utilized to implement ActiveX (Dadkhah et al., 2014). These controls can perform most of the same functions as Java applets except that they do not run in sandboxes and hence have complete access to the computer, including the operating systems and hard drives. They can therefore be used by attackers or hackers to wreak more havoc, such as deleting or stealing files from computer hard drives, as well as formatting the hard drives. Signing ActiveX does not guarantee trustworthiness. The person who signed the control may not have taken time to assess all of the security vulnerabilities which could pose a threat to users and their computers. The main defense against ActiveX controls is to disable them in web browsers. The downside, however, is that some webpage functionality will be lost, such as the inability to run certain web applications or visit certain websites altogether (Bouguettaya & Eltoweissy, 2003; Ciampa, 2008; Joshi et al., 2001).

Cross Site Scripting (XSS) is a mechanism that involves using JavaScript on the victim's computer to extract information and transmit it to an attacker. A malicious code is usually inserted into a dynamic webpage in this type of attack. The intent is not to attack the webpage or web server itself, but to obtain information from an unsuspecting web surfer. Hence, cross site scripting takes the form of social engineering to trick users into performing actions that otherwise should not be performed (Ciampa, 2008; Hydara, Sultan, Zulzalil, & Admodisastro, 2015).

Insider Attacks are other forms of attacks that are on the increase. The FBI and the Computer Security Institute (CSI) reported that insider attacks account for the most losses in

organizations. Seventy-one percent of organizations interviewed said that they had detected various kinds of insider attacks. Insider attacks usually come in the form of privilege escalation and disgruntled employees, as mentioned earlier. People escalate their security privileges on the system to gain unauthorized access to information (Ballmann, 2015; Harris & Hunt, 1999; Joshi et al., 2001).

Push technology is employed by many sites to deliver content to clients. An attacker or even the content provider can take advantage of this to exploit vulnerabilities in a browser to deliver malicious executable code to users. This same vulnerability can be exploited to cause denial of service attacks by overwhelming systems by sending a high volume of information to servers (Basu & Kanchanasut, 2015; Joshi et al., 2001).

Phishing Attacks/Malicious Software are new tricks employed by attackers to gain/steal information from unsuspecting people. One of the most popular phishing techniques is called spear-phishing. This takes the form of unsolicited emails sent to people who have access to sensitive network/computer system information. These emails are authored to appear to be legitimate. Once the victim clicks on them, malicious code or software attached to the emails is installed on the victim's computer to steal sensitive information. This information can then be used to stage an even more sophisticated and damaging attack on the victim's computer system (G. Smith, 2012).

Fake Antivirus Software is another type of malicious software that is on the rise. Fake antivirus software mimics legitimate antivirus software and displays misleading information about non-existent viruses. This is done to trick users into purchasing the commercial version of such software programs in order to remove these non-existent viruses. Once the unsuspecting user provides a credit card number, not only is the person sold fake antivirus software, but the person's

credit card information is also stolen. The software can then be used in most cases as a back-door to get into the victim's computer at will to steal other personal information. The software can also be used for other malicious purposes like taking over the user's computer and using it as a source of distributed DoS attack. This is a multibillion dollar industry operated mainly from European "partnerka network affiliates" networks with different pseudonyms, with each affiliate netting over $130 million annually (Huang, Siegel, & Stuart, 2018; Joshi et al., 2001; G. Smith, 2012; Stone-Gross et al., 2011),

5.4 THREATS FROM SOCIAL NETWORKS

Social networking software has been defined as "online spaces that allow individuals to present themselves, articulate their social networks, and establish or maintain connections with others" (Cain, 2008). Social networking sites such as Facebook, Instagram and Twitter are very popular with people, especially the younger generation. This increase in patronage and other advantages, such as being able to reach a mass audience all at once, has prompted businesses and various organizations to incorporate these social networking sites into various parts of their businesses (Garcia-Morales, Martín-Rojas, & Lardón-López, 2018). It is a well-known and publicized fact that even the US president and the Pope have Facebook and Twitter accounts. Eighty to ninety percent of US college students have accounts on Facebook, the preferred social networking site among that group. Facebook is said to be the most popular social media platform, with more than 2 billion monthly active users as of the second quarter of 2018 (Coco et al., 2018).

Most social network users trust the friends that they make on social network sites. They share large volumes of private information like demographic information, contact information, comments, images and videos (Cain, 2008; Gross & Acquisti, 2005; Gunatilaka, 2011). Most people visit social networking sites to make friends, and then accept friendship requests very easily. In a recent study done at Carnegie Mellon University involving the download and analyses of Facebook profiles, it was found that less than 1% of Facebook users changed their default P&S settings. Most users provided large volumes of personal information like phone numbers (39.9%) and current residence (50.8%), with the majority mostly unaware of or unconcerned with limiting access to private information on their profiles (Cain, 2008). This website has therefore become a "pot of gold" for highly sensitive data.

It is this massive user base and large volume of data shared among these unsuspecting users that has aroused the attention of attackers. Even though most social networking sites have put security measures in place to combat ever increasing security threats, attackers are using trickery and more sophisticated mechanisms to attack users (Chambers, Fry, & McMasters, 2018; Gunatilaka, 2011; Irani, Balduzzi, Balzarotti, Kirda, & Pu, 2011). Cybercriminals have also capitalized on the ease of access to social networks to employ social engineering and reverse social engineering (RSE) to gain exclusive access to people's sensitive information. Both social engineering and RSE are invoked as the first step in more sophisticated attacks. They are used to gain access to users' context information (user specific information or identifying information) which can then be used to launch various attacks like phishing, spamming, and malware on unsuspecting users. The difference between the two approaches is the mode of attack. In RSE the user is normally not directly approached by the would-be attacker. Instead, users are influenced to

perform an action (e.g., click on a link) or tricked to initiate contact with the attacker (Djenouri et al., 2005; Gross & Acquisti, 2005; Gunatilaka, 2011; G. Smith, 2012).

RSE involves three main attack methods: recommendation-based RSE, demographic-based RSE, and visitor tracking-based RSE (Algarni, Xu, Chan, & Tian, 2014; Gunatilaka, 2011; Irani et al., 2011). Recommendation-based RSE attacks victims by exploiting the friend recommendation feature of social networking sites. Demographic-based RSE also uses the friend recommendation feature. Here, the attacker gains access to the user's demographic information such as location, interests, and date of birth. This information can then be used to attack the user in various ways, such as impersonating the user or creating another account on a different social media environment and attacking the user's friends to gain access to more information. Visitor tracking-based RSE, as its name suggests, is based on the visitor tracking feature on some social networks. This allows users to track who has viewed their profiles. This is a useful feature since most people would probably want to know who has viewed their profiles. Attackers, on the other hand, use this function to attract people to their profiles to initiate contact. This allows them to gain information from the visitors, which is later used to attack them.

As mentioned earlier, overwhelming patronage coupled with the aggressive attack methods of attackers has brought P&S issues to the forefront, especially in the cyber environment. User anonymity or user identity is critical in any discussions of privacy in social media. Having access to information without knowing to whom the information belongs is of little use to an attacker. Being able to associate a name or put a face to the information is what adds value to the information. Since most users of social networking sites use their real names to set up their accounts, their identity is exposed to other users. Some search engines index individual social network accounts and make them searchable. Therefore, if an attacker knows a person's name, he

or she can easily obtain the person's profile information (Chambers et al., 2018; Gambs, Killijian, & del Prado Cortez, 2014; Gunatilaka, 2011; Irani et al., 2011). Other ways attackers can expose an individual's identity on social networking sites are by de-anonymizing personal information and using neighborhood attacks (Bilge, Strufe, Balzarotti, & Kirda, 2009; Gambs et al., 2014; Gunatilaka, 2011; Sharad & Danezis, 2014).

People who share the same interest can form distinct groups on social networks to facilitate exchange of information and ideas. An attacker can exploit this by using a combination of group membership information and other history-stealing techniques to reveal the identity of social network users (Chambers et al., 2018; Gunatilaka, 2011; Irani et al., 2011; Sharad & Danezis, 2014). The only information needed to facilitate this type of attack is the user's group information, which typically includes group name, username, date of birth, and other information about members in the group. Attackers are known to focus on social network groups because it gives them access to more information. History-stealing techniques are used to obtain URLs to websites that a user has visited in the past in order to find out the victim's group information (Gunatilaka, 2011; Wondracek, Holz, Kirda, & Kruegel, 2010). The attacker first gains access to the victim's browsing history, which is then scanned and analyzed to find out the victim's group.

Client-side scripting like JavaScript, mentioned earlier, and conditional logic in Cascading Style Sheet (CSS) are some of the methods that can be employed to steal URL link history information (Ciampa, 2008; Gunatilaka, 2011). Most social networks also provide mailing lists of users. Attackers can use these mailing lists to look for profile information of victims or to spam them.

5.4.1 Neighborhood Attack

Social networks can be denoted by a social graph, with users representing a node on the graph as shown in Figure 3. An edge is used to link two people who are close friends. Neighborhood attacks involve the attacker using information about a victim's (node or Vertex) neighbors to identify the victim's (node) and leak the user's privacy (Chambers et al., 2018; P. Wang, Zhang, & Huang, 2015; Zhou & Pei, 2008). For example, user A in Figure 3 has five friends (users B, C, D, E, F); user's B and C are also friends, but D, E, and F are not friends. If an attacker knows that A has two close friends who are also friends and three other friends who do not know each other, this information can be used to identify A and breach his or her privacy. This is because the 1-neighborhood graph of A is unique to A; that is, no other vertex has the same 1-neighborhood graph (Gunatilaka, 2011; P. Wang et al., 2015; Zhou & Pei, 2008).

5.4.2 De-Anonymization Attack

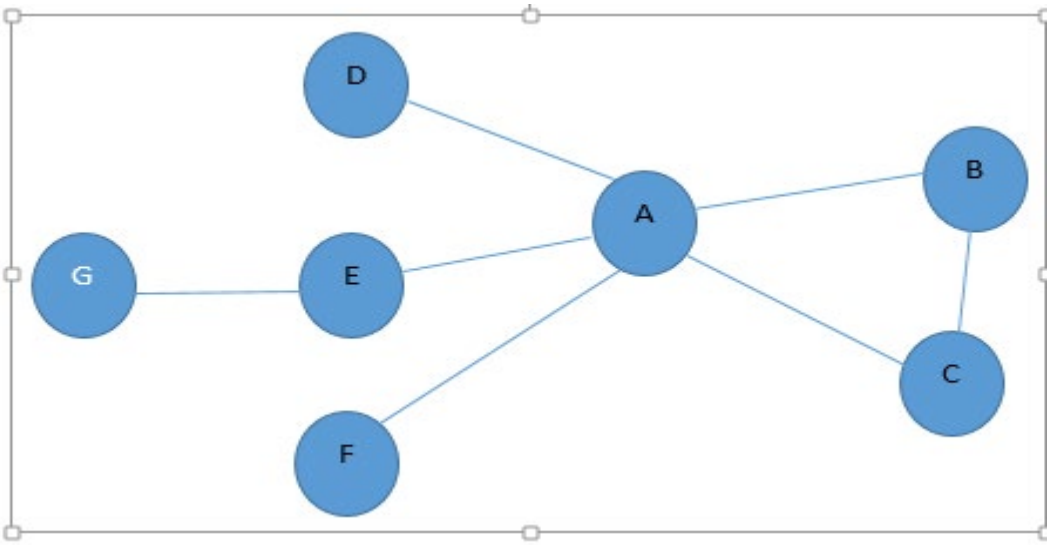

Figure 3: 1- Neighborhood Graph of A

Because almost all Facebook users (>99%) do not bother to change the default privacy settings, their individual profiles are a source of much personal and sensitive information such as full names, contact information, relationship status, date of birth, previous and current addresses as well as educational background. When this personal information is leaked by compromising users' profiles, an attacker can use this to launch more attacks. There are several ways that users' profiles can be leaked:

5.4.3 Inadequate Privacy Settings

Most social network sites use default privacy or permissions of "friends of friends." This means that a person whom a user does not know can gain access to sensitive or personal information by

virtue of the fact that that person is a friend of their friend (Cain, 2008; Watson & Rodrigues, 2018). Attackers can still find ways to circumvent even the strictest privacy settings to steal personal information.

5.4.4 Third Party Applications

Third party developers use application programming interfaces (APIs) provided by social networking sites like Facebook and Twitter to develop applications that run on such platforms. Users allow access to their personal information by these third party applications (Abdulhamid, Ahmad, Waziri, & Jibril, 2014; Balebako, Marsh, Lin, Hong, & Cranor, 2014; Kelley et al., 2013). This usually happens during application setup. Users are typically asked if they want the applications to access their personal data. In other instances, users receive a generic warning that the software will access personal information. Most users are so intent on getting and installing the apps that they do not pay attention to these messages about privacy. These applications can then be used to obtain people's personal data and perform various activities on the user's behalf without the user's knowledge. The information obtained is also sometimes shared with other third party vendors without the user's knowledge (Gunatilaka, 2011; Kelley et al., 2013; Krishnamurthy & Wills, 2008).

5.4.5 Information Leakage to Third Party Domains

This is the use of a third party domain service which most social networking sites employ to track users' activities, mostly for commercial benefit (Pan, Cao, & Chen, 2015). Some social networking

sites partner with different companies (usually advertising companies) to access, aggregate, and analyze users' social networking data for commercial purposes, such as targeting specific advertisements to the users (Gunatilaka, 2011).

Apart from the social engineering attacks discussed earlier, there is the issue of identity theft. This involves using someone's (usually stolen) information to impersonate the person. One common or basic technique used by rogue people to commit identity theft on social networking sites is profile cloning. Another is social phishing.

5.4.6 Profile Cloning

Attackers take advantage of trust among friends on social networking sites and individuals' general lack of care when accepting friendship requests to gain access to personal information. The most vulnerable to this type of attack are those who set their profiles to be public. This allows attackers to access their profile information in order to set up a false social network profile/identity (Gunatilaka, 2011; Meligy, Ibrahim, & Torky, 2015). The two main types of profile cloning are existing profile cloning and cross-site profile cloning (Bilge et al., 2009; Gunatilaka, 2011; Kelley et al., 2013; Kontaxis, Polakis, Ioannidis, & Markatos, 2011).

5.4.7 Existing Profile Cloning

This involves impersonations of social network users by using their biographic information such as name, picture, and other personal information to create another account. The attacker then sends friend requests to individuals known to the user. The strength of this type of attack is that most

users will accept friendship requests from people they know. This then permits the attacker to access personal information of friends of friends (Kontaxis et al., 2011; Meligy et al., 2015; Wondracek et al., 2010).

5.4.8 Cross-site Profile Cloning

This is a more sophisticated attack strategy than existing profile cloning. In this case, the attacker uses personal information stolen from another social networking site to create an account on a social networking site that a user has never visited. This type of account looks even more legitimate in the sense that there is no duplicate account on this new social networking site. The attacker can then send invitations or friendship requests to people on the user's contact list extracted from the previous social networking site. Once the "friends" accept these requests, the attacker can gain access to their profiles(Meligy et al., 2015).

5.4.9 Phishing on Social Networks

Phishing on social networking sites is another issue that users should understand. Phishing involves the use of illegitimate means to extract information from unsuspecting victims (Ciampaglia et al., 2015). Until recently phishing was implemented in the form of unsolicited emails (Smiths, 2012). Phishing has become more sophisticated, with attackers using fake websites that look authentic to fool victims into providing personal and confidential information like passwords, financial information, and various forms of identification information (Gunatilaka, 2011; Halevi, Memon, & Nov, 2015). Phishing can also be in the form of malicious software such

as fake antivirus software that asks users to buy a full version of the antivirus software after the software is purported to have found “fake viruses.”

5.4.10 Social Network Spam

This type of spam usually comes in the form of unsolicited emails. People have become quite aware of spam and will usually delete these emails or use spam filters for protection. Spam on social networking sites, on the other hand, can be introduced in the form of wall posts, news feeds, and other messages that target victims. This spam often contains advertisements and hyperlinks that redirect users to phishing websites when clicked. The context-ware attacks can take three forms which have a high click rate because they look authentic (Brown, Howe, Ihbe, Prakash, & Borders, 2008; Gunatilaka, 2011; He, Lee, & Whinston, 2014):

5.4.11 Relationship-based attacks

These attacks use friend-to-friend relationship information and no other information from the user’s profile to attack. An attack is usually in the form of a social networking contact or email, which serves as a believable medium for launching an attack (Chadwick, 2014).

5.4.12 Unshared-attribute attacks

These malicious attacks use information gained from friend-to-friend relationships, in addition to some type of attribute from one of the persons in the relationship to launch an attack. About 87% of social network users include their birthday on social networks (Brown et al., 2008). An unshared

attribute attack, for example, could present in the form of a “birthday greeting attack” in which the attacker sends an electronic birthday card with embedded malicious code to one of the friends in the relationship. The greeting has to be sent close to the person’s birthday for it to look authentic (Brown et al., 2008).

5.4.13 Shared-attribute attacks

These attacks involve the use of an attribute that is visible to all parties in a “friend-to-friend relationship," such as a common school that both attended (Krombholz, Hobel, Huber, & Weippl, 2014).

5.4.14 HTTP Session Hijacking Attacks on Social Networking Sites (SNSs)

HTTP Session Hijacking Attacks on SNS are usually manifested in the form of a man-in-the-middle attack used to obtain context information from users and their friends. This information can then be used to spam victims and their friends (I. Das, 2014; Gunatilaka, 2011). A variant of the man-in-the-middle attack used on SNSs is a friend-in-the-middle attack (FITM), which has been described as an active eavesdropping attack on SNSs (Huber, Mulazzani, Weippl, Kitzler, & Goluch, 2011). A user’s social networking session can be hijacked by an attacker, allowing the attacker to steal personal information from the victim’s profile (Grunin, Nachman, Nassar, & Nassar, 2015). This information can then be used to spam and send phishing emails to the victim’s friends (Huber et al., 2011). Friend-in-the-middle attacks can also start as eavesdropping. The attacker sniffs a communication/session between SNSs that are not using data encryption and thus

are more vulnerable to these types of attacks. The attack can take different forms: Address Resolution Protocol (ARP) cache poisoning or Domain Name Service (DNS) poisoning (Grunin et al., 2015; Huber et al., 2011). In ARP cache poisoning, the attacker sends forged ARP requests and reply packets which allow the attacker to change the MAC address of the victim's computer to one that the attacker can monitor. The attacker is then able to steal sensitive and private information such as profile information, passwords, and contacts that in turn spam or initiate phishing attacks on the victim's friends (Gunatilaka, 2011; Huber et al., 2011). Most websites employ cookie-based authentication (Ciampa, 2008). An attacker can therefore capture HTTP headers containing session cookies, which can, in turn, be used to access the victim's profile and other personal/private information. The attacker uses information obtained from the sniffing attack to access the victim's profile, which it uses to steal information such as email addresses from the victim's friends to use against them (Gunatilaka, 2011).

5.4.15 Malware/Viruses

Malware such as viruses and other malicious applications also exist in the social networking environment. The spread of viruses in the social networking world is facilitated by the very nature and strength of the system itself. The system relies on the relationships among friends, making it easier for malicious software to be spread across the SNSs. Another weakness of SNSs is their inability to determine if embedded links or URLs are legitimate or not. This weakness can be exploited by attackers who provide fake links on SNSs. When users click on these links they are either redirected to malicious websites to execute a malicious program, or to install malicious

software on their computer in order to steal information from victims and, in many cases, their friends (Gunatilaka, 2011; Kumar & Rani, 2014; Mittal & Singh, 2014).

5.4.16 Drive-by Download Attack

This is defined as an attack in which the user's browser is exploited and malicious software or code are downloaded onto the user's computer without his or her knowledge (Sood & Enbody, 2011). Also known as advertising, this type of attack involves the use of an advertisement to spread malware and other malicious applications across SNSs. Victims are usually redirected to malicious websites after they click on advertisements posted on their walls by attackers. In other instances, malicious code or software is directly installed on the victim's computer when he or she clicks on the advertisements (Gunatilaka, 2011; Kim, Yan, & Zhang, 2015; Sood & Enbody, 2011). Facebook was reportedly hit by a drive-by-download attack that was traced to a group with ties to a certain Facebook application (Gunatilaka, 2011).

5.4.17 Cross-Site Scripting Attack

As described earlier, cross-site scripting (XSS) involves the insertion of JavaScript on the victim's computer to steal information. The attacker injects malicious HTML code into a dynamic website to make the browser send the victim's cookies, which contain personal information, to the attacker's server (Ciampa, 2008; Gunatilaka, 2011; Householder et al., 2002; Lepofsky, 2014). An example is the XSS worm that propagates amongst users who patronize malicious websites. This exploits the "connectivity characteristics" among social network users to spread malicious

software which is then used to steal information. For instance, the attacker identifies a social network user to start the spread of a virus. Once the user logs on, the malicious code takes over the user's browser and performs various activities in the user's name. These include but are not limited to stealing the user's contacts and posting or sending messages to the user's wall. (Gunatilaka, 2011). The contacts can then be used to send or spread malware to the victim's friends.

5.4.18 Clickjacking

Clickjacking is a technique that tricks victims into interacting with an object on a webpage. It can take the form of a web framing attack where an attacker employs iframes to hijack a user's web session (Rydstedt, Bursztein, Boneh, & Jackson, 2010; Shahriar & Devendran, 2014). There are different forms of clickjacking attacks. In some instances, a victim is presented with a video that looks like a real YouTube video. When the user clicks on the video, a malicious code is embedded in the video or a Facebook-like button is executed. This can then be used to access the user's personal or private information. It is easy to spread this malicious code or malware to the victim's friends once some type of profile or context information has been compromised. Sometimes the victim is asked to provide some information before viewing the video. (Gunatilaka, 2011; Rydstedt et al., 2010).

In a typical clickjacking attack, the victim's site is framed in a transparent iframe. This iframe is put on top of another page that looks like a normal or legitimate page. The idea is to deceive the victim into clicking or interacting with the iframe which is, in fact, interacting with the attacker's page (Rydstedt et al., 2010).

Some examples of social network malware are Twitter Worm and Koobface (Gunatilaka, 2011). Koobface is very prominent on SNSs like Facebook. Its main form of propagation is through messages exchanged between friends, often in the form of a video, button, or iframe that entices the victim to click or interact with the object. Twitter Worm, on the other hand, is spread by tweeting a link to a friend, inviting him or her to download some type of application. This could be a third-party application like "Profile Spy," which is supposed to help users to find out who has viewed their profile. Instead, the software steals the victim's private or personal information provided before downloading and installing the software. This allows the attacker to gain access to a host of personal data or confidential information.

5.4.19 Physical Threats

Social media threats can easily lead to physical threats. Victims do not only have to worry about online threats, as some can actually result in physical threats such as stalking (Gunatilaka, 2011; Van Royen, Poels, Daelemans, & Vandebosch, 2015). The personal information that people post on their social network pages can be used to identify them, allowing criminals to find out where they live and either stalk or harm them in different ways. Location-based services on smartphones such as Google latitude or Foursquare can allow criminals to track victim's behavior and location.

As can be seen from these multiple examples, social network patronage must be done carefully for users to safeguard themselves against attacks. Particular attention should be concentrated on reducing the potential for such attacks before using the medium to provide healthcare services of any kind (e.g., healthcare support groups, information about diseases during epidemics, posting educational videos).

5.5 CLOUD BASED SYSTEMS

Cloud computing is basically a way for computer users with varying backgrounds to share a range of computer resources (Abdelmaboud, Jawawi, Ghani, Elsafi, & Kitchenham, 2015; Bele, 2018; Mell & Grance, 2009). The backbone of cloud computing is virtualization. This allows organizations to create and manage their IT infrastructure in a shared environment provided by a third party company, mostly over the Internet (Christodorescu, Sailer, Schales, Sgandurra, & Zamboni, 2009). Cloud computing has been defined as *"a style of computing where massively scalable IT-enabled capabilities are delivered 'as a service' to external customers"*(Dhanalakshmi & Thomas, 2015). Factors driving the adoption of cloud computing by most companies include but are not limited to the cost of procuring and maintaining robust and powerful IT infrastructure or systems (Chou, 2015; Gangwar, Date, Ramaswamy, Irani, & Irani, 2015; Shankar & Duraisamy, 2018). Some of the financial incentives for the adoption of cloud technology are: 1. reduced hardware costs, as companies do not have to invest in high-end computer devices like servers; 2. reduced license costs; and 3. reduced patch management costs. Companies can also save much more money by not having to engineer and manage their own data centers for optimum performance. Cloud computing can also help companies save money from poor utilization of IT resources, as companies only pay for the resources they currently need and can scale up or down as needed. This helps to reduce the tendency of over or under-budgeting for IT resources (Jensen, Schwenk, Gruschka, & Iacono, 2009).

Most small and medium-sized businesses are taking advantage of sophisticated, robust, and powerful high-end business applications offered over the cloud to drastically boost their IT infrastructure at bargain prices (Subashini & Kavitha, 2011). In fact, the US government was

projected to account for approximately 40% of the growth in cloud computing, at a cost that was expected to surpass $7 billion in 2015 (Kaufman, 2009).

Cloud computing is touted to become the next big area in information technology due to its overwhelming advantages such as: on-demand self-service, ubiquitous network access, location independent resource pooling, rapid resource elasticity, usage-based pricing, and transfer of risk. Companies are also relieved of the burden of storage management, capital expenditure on hardware and software, and personnel maintenance (Chou, 2015; Shankar & Duraisamy, 2018; C. Wang et al., 2010).

Even though there are many advantages to cloud computing, it also comes with new and very perplexing security issues (Danish & Sharma, 2018; Lian, 2015; C. Wang et al., 2010; Wei et al., 2014). Users and companies must relinquish definitive control over their data in the cloud to the service providers. No one is sure what third-party companies can or will do with all these sets of data that they control or manage. This poses P&S risks to individuals' data and jeopardizes data integrity (Danish & Sharma, 2018; Kaufman, 2009; C. Wang et al., 2010). With users' data hosted on servers belonging to third party companies who provide cloud services, traditional cryptographic methods for data security become almost impossible to implement (Jensen et al., 2009; C. Wang et al., 2010).

Due to the complex nature of securing data in the cloud, most companies are employing the services of third-party auditors to help with data security(Lins, Schneider, & Sunyaev, 2018). The companies rely on security reports from these third-party auditors to evaluate and address security vulnerabilities in their cloud data. This auditing process has the potential to introduce an additional source through which users' data could be compromised. The potential for information leakage by the third party auditors could create even more problems, especially for healthcare

providers trying to meet data privacy and security standards set by HIPAA/HITECH and other healthcare regulations (Rathi & Parmar, 2015; Rimal, Choi, & Lumb, 2009; C. Wang et al., 2010).

Cloud technology by its nature, therefore, presents significant challenges for healthcare providers who want to adopt the cloud to meet HIPAA P&S requirements. The storage of patient information in the cloud may infringe on certain state and federal P&S requirements (Sotto, Treacy, & McLellan, 2010; C. Wang et al., 2010). Both HIPAA and HITECH regulations have restrictions for both CEs and their BAs to safeguard the P&S of their patients' data (Pasquale & Ragone, 2014; Peterson & Watzlaf, 2015; D. J. Solove & Hartzog, 2014; Sotto et al., 2010). Cloud service providers and healthcare providers must enter into Business Associate Agreements to safeguard the security and privacy of patient data line PHI (F. A. Pasquale & T. A. Ragone, 2013). It is therefore a good idea for companies, especially healthcare providers and their BAs, to have a good understanding of cloud computing. This will make it possible for CEs and their BAs to formulate policies and procedures to protect patient data residing in the cloud, and to make sure that they are in compliance with all the necessary regulations (F. Pasquale & T. A. Ragone, 2013). Another very important policy that providers must contend with is the General Data Protection Regulation (GPRA). It is said to be the biggest shakeup in data protection laws in 20 years (Wilkinson, 2018). Hence health application developers and healthcare providers who intend to use cloud services have to also take GPRA requirements into account when formulating or designing their P&S policies (Wilkinson, 2018).

For the most part, cloud computing comes in three main flavors: private, public, and hybrid (Bele, 2018; Rimal et al., 2009; Ryan, 2014). Each of these flavors has its own advantages and disadvantages:

Private Cloud: The data resides in the company's website. It is under full control of the company's IT staff and therefore not exposed to the same security vulnerabilities and requirements of public clouds. This, however, could limit users' access to the data stored there.

Public Cloud: This is probably the most comprehensive definition of cloud computing. This form of cloud computing usually involves a third-party providing services over the Internet to subscribed users, enabling them to dynamically share resources.

Hybrid Cloud: This is a combination of the private and public cloud and is made up of internal and external providers.

There are different forms of cloud services such as application/software and platform, hardware and infrastructure as a service.

5.5.1 Software-as-a-Service (SaaS)

This is otherwise known as the Application Service Provider (ASP) model and entails use of shared resources to make applications/software and associated databases available to users (Bele, 2018; James & Chung, 2015; Rimal et al., 2009; Ryan, 2014; Subashini & Kavitha, 2011). Companies including healthcare providers do not have to spend large sums of money to buy these software/applications, including the annual license and support fees (Jensen et al., 2009; Subashini & Kavitha, 2011; F. Zhao, Gaw, Bender, & Levy, 2018).

5.5.2 Platform-as-a-Service (PaaS)

This service is offered mainly for developers and programmers. It enables them to remotely access resources and tools needed for various aspects of the software development cycle. These include but are not restricted to developing, testing, deploying, and hosting sophisticated web applications (Bele, 2018; James & Chung, 2015; Rimal et al., 2009; Subashini & Kavitha, 2011).

5.5.3 Hardware-as-a-Service (HaaS)

The days of "personal computing" as it is known now are almost over (Carr, 2013; Shankar & Duraisamy, 2018). Most companies are not relishing buying or owning their own computer hardware or resources. Instead, they are shifting towards the use of HaaS (Bouzidi, Soltani, Bouhank, & Daoudi, 2018; Carr, 2013; James & Chung, 2015; Sotto et al., 2010; C. Wang et al., 2010). More and more companies are adopting pay-as-you-go subscription services that scale up or down according to their needs for IT hardware (Shankar & Duraisamy, 2018). HaaS has numerous advantages such as flexibility, scalability, cost and place independence. IT administrators do not have to worry about maintenance (system updates, software patches and disaster recovery) as these services are provided by the service providers (Bouzidi et al., 2018; Shankar & Duraisamy, 2018). Hence some corporations have even gone as far as using this type of service to set up complete data centers (Shankar & Duraisamy, 2018).

5.5.4 Infrastructure-as-a-Service (IaaS)

Companies can build their whole IT infrastructure on a pay-as-you-go basis. This gives them the flexibility of paying for what they use as well as having the newest technology at their disposal. Most companies are starting to find this model very economical (Bele, 2018; James & Chung, 2015; Rimal et al., 2009; C. Wang et al., 2010).

On the average, the United States healthcare expenditure is projected to grow by 5.5% annually in 2017 to 2026. This will be 19.7% of the U.S. economy.(Cuckler et al., 2018) Healthcare providers including hospitals are looking for ways to cut costs. Adoption of cloud computing technology can lead to tremendous reduction in IT budget (Ali, Shrestha, Soar, & Wamba, 2018). This will require strict rules and procedures to be put in place to meet all HIPAA/HITECH and state regulations. Some of the data P&S issues pertaining to cloud computing are discussed here.

5.5.5 Browser Security

Because cloud computing is primarily done over the Internet, it is subject to most of the security issues of Internet browsers (Jensen et al., 2009; Mahajan & Giri, 2014; Shankar & Duraisamy, 2018). These include Cross Site Scripting (XSS), ActiveX, JavaScript's, and the malicious web applications discussed earlier.

5.5.6 Availability

Reliance on the cloud could cause significant availability problems due to downtime and outages that are out of an organization's control. An attacker can use a flooding attack, which involves sending large volumes of nonsense data to the cloud. This could overwhelm the system and make it difficult for the system to respond to legitimate requests, thus leading to Denial-of-Service attacks (Danish & Sharma, 2018; Grover & Sharma, 2014; Jensen et al., 2009). Summaries of downtime by some cloud service providers can be found in Table 6 (Addo, Ahamed, & Chu, 2014; Mesbahi, Rahmani, & Hosseinzadeh, 2018; Rimal et al., 2009; Srinivasan, 2014; Subashini & Kavitha, 2011). Such downtime poses significant problems with the parts of HIPAA and other healthcare legislation that deal with data availability. An example of non-availability of data could arise when, for instance, a patient has to be treated but physicians and other healthcare workers are not able to access their PHI residing in the cloud that is required to make decisions (Mxoli, Gerber, & Mostert-Phipps, 2014; Mxoli, Mostert-Phipps, & Gerber, 2017).

Table 6: Outages in Different Cloud Services

Service and Outage	**Duration**	**Date**
IBM's cloud infrastructure failure	Several hours	January 26, 2017
GitLab's popular online code repository service outage	Several hours	January 31, 2017
Facebook		February 24, 2017
Amazon Web Services	~ 4 hours	February 28, 2017
Microsoft Azure	7 hours	March 16, 2017
Microsoft Office 365	Several hours	March 21, 2017
Microsoft Azure: Malfunction in Windows Azure	22 hours	March 13-14, 2008

Table 6 (continued)

Gmail and Google Apps Engine	2.5 hours	Feb 24, 2009
Google search outage: programming error	40 min	Jan 31, 2009
Gmail: Site unavailable due to outage in contacts system	1.5 hours	Aug 11, 2008
Google AppEngine partial outage: programming error	5 hours	June 17, 2008, October 26, 2012
S3 outage authentication service overload leading to unavailability	2 hours	Feb 15, 2008
S3 Outage: single bit error leading to gossip protocol blowup	6-8 hours	July 20, 2008
FlexiScale: core network failure	18 hours	Oct 31, 2008
Amazon: Amazon Website Outage, caused by a glitch in backup system	3 days	April 21, 2011
Amazon: Amazon Website Outage	-	Sept 13, 2013
Gmail outage:	Few minutes	April 17, 2013
Microsoft Outlook Services: caused by firmware updates that affected temperatures at data centers	16 hours	March 14, 2013
Facebook	2 hours	January 28, 2013
PayPal: Internal network problems	Several hours	August 3, 2009
Healthcare.gov	Several hours	October 2013

5.5.7 Cloud Malware Injection Attack

This type of threat to privacy and security is generally manifested in the form of SaaS or PaaS. The attacker creates his or her own malicious service implementation model. This could be a virtual machine instance (IaaS), SaaS, or PaaS and added to the cloud system. The rogue person

then must trick the cloud system into accepting the new (malicious) instance as one of its legitimate instances of the service he or she is looking to attack. Once this is accomplished, the cloud system automatically redirects the user request to the rogue service implementation. The malicious code incorporated into the service then executes once users connect to the service (Akshay, Kakkar, Jayasree, Prudhvi, & Metgal, 2015; Dhote & Bhavsar, 2018; Jensen et al., 2009). This could be used to access a patient's sensitive data if a healthcare provider were using this service for patient care.

5.5.8 Data Encapsulation and Data security

If the right security measures are not put in place to segregate patient data, multiple users could see each other's data (Ali et al., 2018; Subashini & Kavitha, 2011; J. Zhao et al., 2014), which would violate HIPAA/HITECH regulations. The right access control, data management, and encryption methodology must be employed to protect users data in the cloud (Usman, Jan, & He, 2017).

5.5.9 Data security

Data security is a major issue in cloud computing. In "traditional computing," a company's data, software, and other applications are within the CE's IT network. These data sets are therefore subject to the CE's physical, logical, and personnel security and access control policies. When data are stored in the cloud, as in the SaaS model, companies must rely on the SaaS vendor for data security (D. J. Solove & Hartzog, 2014; Subashini & Kavitha, 2011; Yinghui Zhang et al., 2017).

They completely give up all security of their data in favor of the vendor's approach. The possibility of a breach is thus very high because the data are on a vendor's system (C. Wang et al., 2010; Yinghui Zhang et al., 2017). Even though these vendors may employ additional security, such as strong cryptography and other measures to protect data and a well-knitted authorization protocol for access control, they still must comply with HIPAA/HITECH and other state regulations. This is mandated by the BA rule of HIPAA/HITECH, as well as state regulations.

There is a huge potential for attackers to use rogue means to gain access to users' data because cloud computing has some of the same vulnerabilities as other Internet applications, such as Cross-site Scripting (XSS), Access Control weakness, OS and SQL injection flaws, cookies manipulation, and insecure storage (Appelt, Nguyen, & Briand, 2015; Subashini & Kavitha, 2011; Usman et al., 2017).

5.5.10 Network Security

In the cloud environment, data are moved between the user's computer and the vendor's system through the Internet, potentially leading to exposure of sensitive data to unintended recipients. SaaS providers must therefore employ strong network cryptography techniques like Secure Socket Layer (SSL) and Transport Layer security to protect data (Jensen et al., 2009; Mxoli et al., 2014; Subashini & Kavitha, 2011; Yan, Rong, & Zhao, 2009). If this is not performed correctly, users and corporations connecting to cloud vendors could be subject to attacks such as man-in-the middle attacks, IP spoofing, packet sniffing, and so forth.

5.5.11 Data Confidentiality Issue

By virtue of its nature and implementation, cloud computing can have very serious consequences for data confidentiality (Goswami & Ravichandra, 2015; Jensen et al., 2009; J. Li, Zhang, Chen, & Xiang, 2018; Subhash, 2014). Even though cloud computing has been in use for some time now, data confidentiality is still a major concern(J. Li et al., 2018). Cloud computing involves sharing of users' data stored on remote servers that belong to third party vendors. These data are then accessed through the Internet and other means. When any organization or entity stores sensitive data in the cloud, P&S concerns may occur(Mishra, Sharma, Sharma, & Vimal, 2018). Therefore, this could be a major issue as healthcare providers explore cloud computing as a means of saving money as well as taking advantage of its immense potential benefits.

5.5.12 Data Breaches

Attackers will be enticed by the volume of information stored by cloud service providers. This is because breaching a cloud vendor's system will give the attackers access to a great deal of sensitive data. Therefore, the cloud has the potential of becoming a gold mine of sensitive data for attackers (Golden, 2009; Lafuente, 2015; Mishra et al., 2018). A survey by the Cloud Security Alliance (CSA) found that data breach is a concern to most stakeholders (Mishra et al., 2018). Data stored in the provider's cloud include very sensitive data hence a breach to the provider's cloud could result in serious HIPAA/HITECH violations (Varghese & Buyya, 2018).

5.6 MULTI-USER HEALTH KIOSKS

Self-service is the capacity for a customer to perform activities related to the provision of a particular service without the intervention of a service provider/personnel (Ding, Verma, & Iqbal, 2007; H.-D. Yang, Lee, Park, & Lee, 2014). Self-service technologies (SSTs) have been used successfully in industries other than healthcare for years. They come in the form of automated teller machines (ATM), computer kiosks to check in for flights, self-service gas stations, self-pay parking meters, booths used in public parking garages, CD rental kiosks at various locations, self-checkout kiosks at various super markets and grocery shops, Internet and cell phone apps and online classes or e-learning, among others.

The main factors driving the adoption of SSTs across all major industries are efficiency and cost savings. Adopting self-service can also give companies a competitive advantage (C.-t. Hsieh, 2015). SSTs allow consumers to participate in service delivery, which enables employees to perform other functions (Burkhart, 2012; Castro, Atkinson, & Ezell, 2010). It appears that users also want convenience and control. Thirty-seven percent of patients surveyed reported that they preferred using self-service kiosks for checking in for their hospital appointments. Another 43% indicated that the availability of SSTs influenced their decision in choosing a healthcare provider (Gaffney, 2009).

The financial impact on the US economy due to the use of SSTs is huge: it is expected to contribute an additional $130 billion. This huge fiscal impact coupled with advanced computer hardware, software, and Internet technology means that we are going to see SSTs in more and more sectors in the service delivery system (Castro et al., 2010). For example, a great many people use kiosks or self-service without even knowing it when they pay bills online or fill their gas tanks.

It is therefore not surprising that the healthcare industry has followed suit. In the health sector, SSTs come in the form of multi-user health kiosks. Persons who have checked their blood pressure at CVS or Giant Eagle have used a form of multi-user health kiosk for health service. Various kinds of multi-user health kiosks have been deployed in hospitals to automate a range of patient services including patient management services for admission, discharge, appointment scheduling, and patient check-in during hospital visits. They can also be used for processing co-payments, patient consent forms, prescription refills, and verification of insurance eligibility. It is also important to note that health kiosks allow hospitals to provide these services in different languages.

Multi-user health kiosks can be used to service many people so long as they have access to the Internet. This is in the form of Internet kiosks. The federal government's healthcare.gov website is one such Internet kiosk which provides access to acquire health insurance to millions of Americans. Healthcare.gov was launched on October 1, 2013 as part of the Patient Protection and Affordable Care Act (ACA). In its initial stages, the website had many flaws. Its fundamental flaws were in reliability and availability, as the website had difficulties coping with the large amount of network traffic from individuals trying to sign up for healthcare coverage (May, 2013; Srinivasan, 2014). The explanation provided for the glitches and bandwidth issues was that the website had to interface with other old legacy government websites and databases. This is said to have created some bottlenecks in the whole system.

Data integrity for healthcare.gov is another concern that has been raised by experts. Some insurance companies have reported receiving inaccurate data. This is a major issue because it could lead to major problems down the road, especially in the continuity of care for patients (May, 2013). Some security concerns have also been reported including claims that the website was vulnerable

to hacking and SQL injection attacks (Appelt et al., 2015). These vulnerabilities were part of 28 unspecified, potential, vulnerabilities uncovered by a company said to have been hired to conduct penetration testing (PENTESTING) on the site (Fung, 2013). Other concerns have been potential threats to other government IT and computer systems with which the website interfaces. Experts are concerned that if healthcare.gov is breached, it will provide an easy gateway into the other government systems with which it interfaces (Fung, 2013).

Despite all of the convenience and cost savings that multi-user health kiosks may provide, there are important P&S issues to consider (Ciampa, 2008; Kizza, 2013b; B. Smith, 2008; Uhley, 2006). The very same characteristics of kiosks that make them attractive for use in the self-service environment could very well make them vulnerable (Günay, Erbuğ, Hekkert, & Herrera, 2014; B. Smith, 2008; Uhley, 2006):

Unattended device: Users can access the devices on their own with little or no supervision. As a special purpose device, a multi-user health kiosk is built to be used to accomplish specific tasks. The systems are mostly tied down by disabling a user's ability to view data entered by other users or to install programs, tamper with various software on the kiosk, or gain access to the operating system and the file system.

Kiosks can be installed almost anywhere. Owing to their almost portable nature, they can be deployed in all kinds of places where users can easily see and access them. They are also connected to some type of network.

Users have few or no restrictions: Most users who patronize kiosks do not need explicit IT or network privileges like user names and passwords. Users usually use some form of generic log-on information, and all users operate by the same restrictions. It is a challenge for system

administrators to manage or track user activities on kiosks and to protect them from numerous security threats.

Physical threats: These could be in the form of hardware threats or threats to the users. Because kiosks are typically available in public but sometimes obscure locations, vandals can vandalize the hardware itself as well as attack the data of individuals who patronize the kiosks. Media devices such as CD-ROM drives and USB ports could be exploited to breach the systems. Hence, there should be absolutely no user or external access to cabling or to any of the internal components of the system such as hard drives and USB and serial ports. Having access to CD-ROM drives and USB ports would allow criminals to install malicious software or devices to compromise a kiosk. Internal components should be situated in secured enclosures to prevent the theft of hardware such as hard drives. Peripheral devices, like keyboards, could allow hackers to install devices like keyboard recorders to record users' keystrokes and to gain access to personal and confidential information. If possible, kiosks should be designed to use touch screens instead of a regular keyboard and mouse. In situations where keyboards are used, special keyboards without function keys should be employed. Steps have to be taken to prevent users from having unrestricted access to the underlying hardware of kiosks. They also have to be deployed in well-lit areas in order to protect the equipment as well as the user.

Threat to users: These threats usually come in the form of identity theft and fraud. "Shoulder surfing" is one way that this can happen. Privacy screens have to be installed in kiosks to make it difficult for anyone to read information off the screen when someone else is logged on.

Threat to the provider's network and computer systems: Cybercriminals can profit from obtaining companies' information as well as users' personal or confidential information. Because most kiosks are deployed on shared networks (i.e., the same network as used for other information

technology services), attackers can gain access to other aspects of a company's network by compromising kiosks on their network. As mentioned earlier, if ports and CD-ROM drives are not confined, malicious individuals could attach via network jacks. This would enable them to attach their own devices to the network to instigate man-in-the-middle attacks as well as other attacks. Kiosks should therefore be deployed on their own dedicated networks to segment them from other networks used by the company. Sub-netting, firewalls and other intrusion prevention systems should be deployed between the kiosk network and other aspects of the company's network to prevent intrusion.

Vulnerabilities due to operating systems and other software: Attackers can bypass kiosk access controls if they are able to gain access to the underlying operating system and file system. Special purpose operating systems, specifically designed for kiosk functions, are deployed on kiosks to prevent users from performing unauthorized functions.

Most attackers find the means to circumvent the operating system access control mechanism. An operating system access control mechanism for a multi-user health kiosk therefore has to be configured to make it difficult to by-pass through what is usually referred to as "reference monitoring," which uses a set of well-defined design requirements to enforce access control mechanisms (Jaege, 2013). However, it is very difficult to tie down systems without losing some of their functionality. A balanced approach to security is therefore the best way to go.

As was mentioned earlier, a multi-user health kiosk system and all of its components should be protected in terms of all the attributes of PHI (B. Smith, 2008).

Kiosks may be exposed to a host of network attacks. The following are some examples of tricks attackers can employ to get around access control mechanisms:

- Most Microsoft applications have Visual Basic (VB) editors built into them. Attackers can activate and use these to write small scripts that could open up loopholes by which to gain unlimited access to the system. For example, using the ALT+F1 key combination in a blank Word document can open up the VB editor for the attacker to use. Similar tricks can be employed in the VI text editor in Linux.
- Browsers offer another way an attacker can gain access to the file systems. Most kiosks have various functionalities of browsers disabled. For example, the address bar of browsers is typically disabled. However, holding down the shift key and clicking on a hyperlink will open up the link in a new browser window, usually with the address bar enabled.
- The calculator is another method an attacker can use to infiltrate a kiosk system. Most Microsoft Windows operating systems contain calculators. Clicking F1 while the calculator application is opened will usually activate the Help function. There is a tap in the Help function labeled 'Jump URL." Clicking on this will open the web browser as well as provide access to other areas of the file system.

Table 7 gives a summary of several different ways to infiltrate, or hack, kiosk systems. These are just a few examples. There are numerous other ways an attacker can get into a kiosk system (Craig, 2008).

Table 7: Some Simple ways to Hack Kiosks

Some Simple ways to Hack Kiosks	
Vulnerability Type	Possible Solution
Access Admin Menu from Windows Shortcut keys	

Table 7 (continued)

CTRL-Esc-F9 CTRL-ALT-F8 ALT-Esc-F10 CTRL-ALT-F5	Disable all windows shortcut keys. An even better solution will be to install a special keyboard with no shortcut keys
C:\windows\ may be blocked. But	Test and block all file browsing capabilities Disable URL entry bar or address bar
File:/C:/windows %HOMESHARE%	
File://C:/windows %APPDATA% %SYSTEMDRIVE%	
File:/C:\windows\ %WINDIR% %SYSTEMROOT%	
%TMP%	
%HOMEDRIVE%	
Keyboard Combinations can produce Dialog	
CTRL-B, CTRL-I (Favorite's) CTRL-H (History) CTRL-L,CTL-O-(File/Open Dialog) CTRL-P - ?(Print Dialog) CTRL-S –(Save As) CTRL-SHIFT-ESC (Task Mgr.) ALT-TAB(Switch Task) CTRL-ESC(Start Menu) Alt-F4 (Close Application shell:::((21EC2020-3AEA-1069-A2DD-08002B30309D))	Use a special driver for kiosk keyboard that disables all shortcut keys
Type the following into URI Bar	
Shell: Profile Shell: Program Files Shell: System	Disable access to the all web browsers on the kiosk
Shell:ControlPanelFolder Shell:windows	Hide or disable address bar of the Kiosk browser or block the shell handler on the Kiosk
Online Tools	Disable the access to the Web.
iKAT –Interactive Kiosk Attack Tool	Use for penetration testing to discover and block security loop holes

Apart from the general security concerns discussed earlier, kiosks present more security concerns when used in healthcare. Examples include:

- Masquerading/unauthorized access: Imposters can use this technique to gain access to user data or escalate their privileges on a network. This is done by gaining unlawful access to another user's credentials through illegal means such as hacking or shoulder surfing.
- Unauthorized use of resources: Unscrupulous users can utilize various illegal means (e.g., privilege escalation, backdoors, rootkit, default accounts and unprotected access points) to gain access to resources on a network or network computers, allowing them access to another user's PHI.
- Unauthorized disclosure and flow of information: As mentioned earlier, once an attacker has access to the kiosk system, by installing network taps or malicious code/applications, he or she can gain access to a host of personal information. This includes information retained on the kiosk or saved on servers and other network devices. Attackers, after obtaining initial information, can engage in further clandestine activities such as man-in-the-middle attacks and denial-of-service attacks (B. Smith, 2008; G. Smith, 2012; Uhley, 2006).
- User errors/forgetfulness: This is the least talked-about P&S vulnerability pertaining to kiosks. What is the consequence if a user fails to completely log out or exit the system after using it? Another person could easily latch onto the un-terminated session and gain access to the user's information or even compromise the entire system (Fei Yu, 2011; Kizza, 2013a).

For multi-user health kiosks to be HIPAA/HITECH compliant and also meet the requirements of other state and federal regulations, procedures must be in place to minimize some

of the P&S threats to kiosks. The main issue with compliance is that there is no clear-cut measure. Kiosk architecture should be designed from the bottom up with HIPAA/HITECH and other regulations in mind. That means that the system must be able to protect or ensure security, privacy, confidentiality, integrity, availability, and non-repudiation of information. Careful attention must also be paid to aspects of HIPAA/HITECH that deal with CEs and BAs. Kiosks' hardware must also comply with the Americans with Disabilities Act (ADA) Section 508 regulations, which set standards for electronic and information technology (Gaffney, 2009). ADA requires that visually impaired as well as physically-challenged people who are restricted to a wheelchair and the visually impaired have equal access comparable to access enjoyed by people with no physical disability (Derek Fretheim, 2008; Gaffney, 2009). This means that an ADA-compatible kiosk must accommodate people with any physical capability and must not hinder their ability to use kiosk peripheral devices such as biometric devices, keyboard, bill acceptor, and blood pressure cuffs.

Healthcare institutions which deploy kiosks that provide access to PHI should always have an attendant available to help the user and generally supervise kiosk usage. Having an attendant available also helps to prevent individuals with bad intentions from tampering with kiosks. There should also be user as well as employee education on P&S issues and procedures. There should be custom-built cabinets to conceal internal components such as CD ROM drives, USB ports, and other peripheral devices. There should also be physical intrusion detection systems in place (alarms). Privacy screens should also be part of the kiosk design to prevent shoulder surfing. The system should be configured to turn off after a period of inactivity to prevent people from latching onto un-terminated sessions. It is important to implement sub-netting with firewalls to separate the kiosk systems from other segments of the healthcare provider's or application vendor's network. Active directory group policies should also be employed to disable all unnecessary functionalities

to help close some of the major security loopholes. The kiosk should also be configured to transmit data in real time in an encrypted, secured manner to a secured server. User data should not be kept on a kiosk. Users' PHI should be stored in segments. Identifying/personal information such as name, date of birth, and address should be stored in a separate database from users' EHRs or PHI. Kiosk manufacturers also have to make sure they incorporate FDA-approved medical devices in their kiosk deployments (Derek Fretheim, 2008; Gaffney, 2009).

6.0 EXTENSION OF THE TECHNOLOGY ACCEPTANCE MODEL

As new technologies are developed or adapted to be used to provide healthcare services to people, it is important to pay attention to factors that contribute to technology acceptance. Much research has been done on the design and implementation of IT in healthcare, but there has not been enough research on how people react to IT products that are already in place (Fox & Connolly, 2018; Holden & Karsh, 2010; Kowitlawakul et al., 2015).

The Technology Acceptance Model (TAM) was developed in 1980 by Fred Davis, specifically to predict and measure the factors that influenced users' acceptance of information technology (IT) (Holden & Karsh, 2010; Kowitlawakul et al., 2015; Maillet, Mathieu, & Sicotte, 2015; Oinas-Kukkonen & Harjumaa, 2018). It was adapted from the Theory of Reasoned Action (TRA) which states that a person's performance of a specific behaviors is determined by his/her behavioral intention (BI) to perform the behavior, and BI is also equally determined by the person's attitude (A) and subjective norms (SN) concerning the behavior in question (Holden & Karsh, 2010; Porter & Donthu, 2006). The two main variables of TAM are:

- Perceived usefulness (PU) – An individual's perception that using an IT system or technology will enhance job performance or improve the method used to accomplish a specific task.
- Perceived ease of use (PEOU) – The extent to which users find the use of a technology to be free from effort on their part.

There are other variables that contribute to TAM. These are:

- Attitude toward using – A user's positive or negative feelings about using a technology.

- Intention to use – The state of mind that drives an individual to use or not use a technology.
- Actual system use – The probability that a user will use a particular technology.

A vital element in TAM is to trace the effect of external influences (i.e., individual differences) on internal beliefs, attitudes, and intentions (Curran & Meuter, 2005; Porter & Donthu, 2006; K. C. Yang, Chye, Fern, & Kang, 2015).

TAM has been modified and extended to ascertain technology acceptance of IT products in different fields such as banking, healthcare, and marketing. Other variables such as "risk" have also been introduced in other models of TAM to investigate the influence that factors relating to those variables have on users' acceptance of different technologies (Curran & Meuter, 2005; Holden & Karsh, 2010; Porter & Donthu, 2006; K. C. Yang et al., 2015). Another example is the model used in a study conducted by Tung et al. in 2008 to study the adoption of the electronic logistics information system in the medical industry. Two research parameters, trust and perceived financial cost, were added to their proposed hybrid TAM model. They found that 'trust,' which has been referred to as "perceived risk" by other researchers, had a great positive influence on 'behavioral intention to use.' 'Perceived financial cost' was found to have a "great negative influence" on 'behavioral intention to use' (Oinas-Kukkonen & Harjumaa, 2018; Tung, Chang, & Chou, 2008).

Researchers in Taiwan used an extension of the Technology Acceptance Model to assess the impact that risk perception plays in technology acceptance. They introduced "perceived risk," defined by the variables security and privacy, into their TAM model (C.-F. Li, 2013; Lin, Featherman, Brooks, & Hajli, 2018). "Perceived risk" of using the system is associated with a perception of P&S and confidentiality (Fox & Connolly, 2018; P.-J. Hsieh, 2015; C.-F. Li, 2013).

Ease of use, usefulness, need for interaction, and risk are the predictors that influence user attitude towards SSTs and subsequently, intention to use. “Perceived risk” was defined as how confidential and safe an individual believed that banking transactions would be on Internet banking systems. Perceived usefulness contributed the most (54.6%) to the explained variance in acceptance of Internet banking technology among customers in Taiwan, followed by perceived risk (33.3%) and perceived ease of use (29.1%). The investigators also found that among those who had used the system for an extended period of time concerns about perceived ease of use declined as the systems became easier to use over time. Hence, perceived risk of breach to P&S is an important factor in determining whether a particular user will continue to use the system or not. For the rest of this paper, perceived risk will be associated with risk of breach to P&S.

Ortega et al. (2011) extended the Technology Acceptance Model with two additional factors, trust and risk, to examine physicians’ acceptance of electronic health care records (EHCR systems) (Ortega Egea & Román González, 2011). The investigators used three main variables (institutional trust, perceived risk, and information integrity) to assess how those variables affected physician acceptance of EHCR. They found trust and risk factors (perceived institutional trust, perceived risk, and information integrity) to be strong predictive factors of physician acceptance of EHCR systems.

Users’ perceived risk has also been reported as a major barrier to adoption of new self-service technologies (SSTs) (Charness & Boot, 2009; C.-F. Li, 2013; Subashini & Kavitha, 2011). To improve user acceptance of SSTs, it is important to reduce perceived risk of breach to P&S because this can improve users’ intentions to use SSTs, which may further result in their actual usage (Curran & Meuter, 2005; Lin et al., 2018).

Miyazaki et al. in 2001 cited P&S as one of the major concerns of online shoppers (Miyazaki & Fernandez, 2001). Also, as far back as the year 2000, the Federal Trade Commission (FTC) saw consumer risk perception as one of the primary obstacles to e-commerce. Therefore, P&S and confidentiality should be made a major part of the development of any technology to be used in the healthcare sector.

Aside from ease of use and usefulness, in addition to P&S concerns, some of the main deterrents to acceptance of HIT among users are lack of perceived benefits, convenience, user friendliness, and trust. (P.-J. Hsieh, 2015; Or et al., 2010). Research has shown that ways to improve trust involve, but are not limited to, improved P&S, confidentiality, availability, and integrity of HITs (Corritore, Wiedenbeck, Kracher, & Marble, 2012; P.-J. Hsieh, 2015).

7.0 STEPS IN DEVELOPING PRIVACY, SECURITY, AND CONFIDENTIALITY CEHCKLISTS AND POLICIES

The Health Kiosk Project at the University of Pittsburgh provides an example of how an audit checklist aimed at mitigating users' P&S and confidentiality concerns has been developed. Funded by the Agency for Health Care Research and Quality (5R01HS022889 PI: Matthews), the project involves several health kiosks that have been designed for use by older adults in community-based congregate settings. The settings include senior centers, subsidized senior housing, and continuing care retirement communities.

Each kiosk consists of a wheeled desk and desk chair, touch screen monitor, RFID reader, printer, and selected medical devices that either require manual entry of measurements (blood pressure monitoring device) or are integrated (hand dynamometer and seated scale) with the on-board computer. The hard drive is encrypted, as are data transferred from the kiosk via MiFi hotspot to secure university servers. A cell phone in the kiosk drawer facilitates users' requests for assistance, and a messaging feature on the touch screen enables textual communication with the project team.

At the kiosk, users self-administer health-related surveys, learn behavioral strategies for improving aspects of their health, and receive graphical feedback depicting their progress toward personal goals related to sleep, bladder control, mobility, and mood, among other topics. Wireless headphones convey voiceover for all content displayed on the touch screen. Relevant educational materials may be printed to take home.

The following steps were implemented to develop an audit checklist for addressing potential P&S vulnerabilities of the kiosks in the Health Kiosk Project:

Investigate and Research Possible Security Vulnerabilities: This step entailed garnering expert opinions from published work, textbooks, and interviews with people involved in the design and development of the system, and from "walking through the systems" (Bishop, 2003; Craig, 2008; Garg & Camp, 2015; Kalaiprasath, Elankavi, & Udayakumar, 2017). Specifically, we drew from the literature, interviews with the project team, and direct interaction with the kiosk. We also used the penetration testing techniques (PENTESTING) specified by Craig (2008) to aid in identifying possible vulnerabilities of our multi-user health kiosk design.

Perform a Risk Assessment: Eight steps were involved in assessing the extent to which P&S could be breached (Oyelami & Ithnin, 2015; Stoneburner, Goguen, & Feringa, 2002; Takyi, Watzlaf, MATTHEWS, Zhou, & DeAlmeida, 2017):

Characterize the System: This step helped to define the scope of the risk assessment by identifying items that needed to be protected. We recognized that a solid understanding of the system's architecture as a whole was needed to successfully complete this step (Garg & Camp, 2015; Oyelami & Ithnin, 2015). Hence, system information was collected and classified as: hardware, software, system interfaces (external and internal connectivity), data and information, individuals who support as well as use the system, main functions of the system (functions performed by the system), criticality of the various components of the system to the organization (e.g., how critical the particular component is to system functionality), and sensitivity of system components. After carefully looking through and analyzing various aspects of the health kiosk system, working with the project team, and using information about P&S for multi-user health kiosks discussed earlier in this paper, we identified areas of the system that needed to be protected. These areas formed the core part of the header for the major sections of our audit checklist.

Identify Threats: Possible threats to the system that could lead to vulnerabilities were characterized as high, medium, or low. Informed by expert opinion, the developer's past experience, and industry trends and standards, we focused on identifying anticipated threats rather than every possible threat, as the latter could have been overwhelming and unrealistic to accomplish (Gribaudo, Iacono, & Marrone, 2015; Oyelami & Ithnin, 2015). We used this process to decide which aspects of P&S were worth protecting. Again, information pertaining to possible threats to kiosks in general, physical interaction with the kiosk during development, and discussions with the project team were instrumental in identifying the sources of threat to our multi-user health kiosk.

Identify Vulnerabilities: Action must be taken to identify the vulnerabilities that can result from threats because vulnerabilities suggest possible weaknesses in the system that can be exploited by adversaries bent on breaching the system. Some of the ways to identify vulnerabilities are system security testing and evaluation, penetration testing, and vulnerability scanning using any type of automated vulnerability testing tool (Rebollo, Mellado, Fernández-Medina, & Mouratidis, 2015; Rinehart-Thompson, 2013). We undertook this step-in discussion with the main developer of the kiosk to identify whether vulnerabilities existed pertaining to password protection, privilege escalation, applications and user authentication, and encryption, to mention but a few.

Control and analysis: This step entail reviewing and analyzing controls that have been implemented or are planned to be implemented, to reduce the probability of a threat or adversary exploiting the system. As part of this step, impact analysis should be performed to determine the impact (i.e., loss of integrity, loss of availability, and loss of confidentiality) to the system in case a vulnerability is exploited. The controls can be technical or non-technical. An example of a technical control would be implementing an encryption strategy to protect data. Non-technical

controls could include personnel training regarding proper methods for reducing the probability of a vulnerability occurring. Means of control should be preventive, deterrent, detective, reactive, and capable of recovery (Rebollo et al., 2015; Rinehart-Thompson, 2013). The Health Kiosk Project team considered the impact that the identified vulnerabilities could have on the functionalities of the kiosk. The team then acted to minimize or eliminate those vulnerabilities that posed the greatest risk.

Determine Likelihood of Occurrence: This step involves estimating the likelihood (high, medium, or low) that a particular vulnerability will occur (Rinehart-Thompson, 2013). The Health Kiosk Project team examined the design and types of activities performed on the kiosk to further decide which vulnerabilities were more likely to occur. This resulted in further streamlining of the kiosk features and functionalities that we wanted to protect to include in our audit protocol.

Determine Risk: Assessing the level of risk to the IT system allows for expression of the level of threat and vulnerability for the pairs that have been identified, the magnitude of the impact in the event that a vulnerability is successfully exploited by a given threat, and determination as to whether adequate P&S procedures have been put in place to reduce the risk (Nazareth & Choi, 2015; Rinehart-Thompson, 2013). For the Health Kiosk Project, we had a series of meetings to discuss how the different vulnerabilities could impact the functionality of the kiosk, including what would happen if there were no backups and data were corrupted or lost in the backend database, or whether there was a redundant power supply in case of power outages.

Recommend Controls: To reduce or eliminate perceived risk, recommendations need to be enacted that are appropriate for an organization's operations, requirements, legislated mandates, and standards. Factors that should be considered during this process include, but are not limited to, effectiveness of the recommended options such as system compatibility, legislation and

regulation, organizational policy, operational impact, and safety and reliability (Rinehart-Thompson, 2013). The Health Kiosk Project team used information gathered in the earlier steps as well as requirements for HIPAA and HITECH compliance to decide the aspects of the OCR audit checklist to incorporate into our final audit checklist.

Document the Result: Threat sources and potential vulnerabilities that are identified should be documented in a report or briefing (Rinehart-Thompson, 2013). For our work, we matched the potential vulnerabilities to the OCR Audit protocol. We then adopted aspects of the OCR audit protocol that match our vulnerabilities to develop an audit checklist for the multi-user health kiosk (Appendix A) which can be used by any developer, researcher, or other user of the health kiosk to make sure that the system meets the P&S provisions.

Specify the Checklist: The audit checklist was then finalized for our kiosk by adapting parts of the OCR audit checklist, a checklist developed by Watzlaf et al., and a Security Self-Assessment Guide for Information Technology Systems that was developed by the National Institute of Standards and Technology (Christiansen, 2013; Swanson, 2001; V. J. Watzlaf et al., 2010; V. J. Watzlaf et al., 2011).

8.0 FACTORS THAT AFFECT TECHNOLOGY ACCEPTANCE BY OLDER-ADULTS

Researchers previously thought that physiological factors and cognitive variables were some of the main factors influencing technology adoption by older adults. However, recent comparisons of Internet usage between older adults and the younger generation suggest that there may be other variables influencing technology adoption rates (Knowles & Hanson, 2018; O'Brien et al., 2008). The Pew Research Center has found that more than half of older adults age 65 and older use the Internet for various purposes: 59% use online applications, 47% have high speed Internet or broadband at home, and 77% have cell phones. However, even though older adults use the Internet, they still lag behind younger adults when it comes to Internet usage (Care-Innovations, 2013; A. Smith, 2014). The number of older adults who use the Internet and broadband drops off sharply around age 75 and above(Mazur, Signorella, & Hough, 2018).

Some of the factors or variables found by researchers to influence technology acceptance/adoption by older adults include but are not limited to:

Physical challenges in using the technology: Many older adults have health and physical conditions that make it uncomfortable to use new technologies. Approximately two out of five older adults have acknowledged physical or health conditions that make simple things such as reading a chore. Some also have a disability or chronic disease that hampers their ability to perform common daily activities (Fischer, David, Crotty, Dierks, & Safran, 2014; Hunsaker & Hargittai, 2018; A. Smith, 2014).

Skepticism about the benefits of new technology: Older adults are usually not sure if the use of a technology will be beneficial to them or not. They will not adopt a new technology unless they see clear benefits of adopting a particular technology (Fischer et al., 2014; Hunsaker & Hargittai, 2018; O'Brien et al., 2008; A. Smith, 2014). Research has shown store kiosks to have about a 60% usage rate among older adults. This finding suggests that older adults will voluntarily adopt new technologies if they find them to be beneficial or, as in this case, convenient (Anthony et al., 2015; O'Brien et al., 2008).

Difficulties in learning to use new technologies: A good number of older adults have indicated requiring assistance in using new technologies or digital devices. Only about 18 % of the adults surveyed said they feel comfortable using new technologies on their own and 77% said they would need assistance in using a new technology (O'Brien et al., 2008; A. Smith, 2014).

Cohort and historical time periods: Perception and adoption of new technologies by older adults also depends on the cohort and historical period in which they grew up. This is explained by the time course theory, which takes into account the cohorts and historical time period influences in adoption of new technologies by older adults (White, 2008). The perceived ease of use and perceived benefit of new technologies by older adults is usually influenced by the cohort in which they grew up. Hence, technology usage by older adults in the United States, especially in healthcare, is expected to increase as over 78 million baby boomers age (Care-Innovations, 2013; Heinz, 2013).

Digital Divide: Older adults lag behind in the use of computer technology compared to adults in younger generations (Jesdanun, 2004; Mazur et al., 2018). Experience with technology declines in older adults age 65 year and older. This is due in part to the lack of access to different types of technologies at earlier stages of their lives (Heinz, 2013; Hunsaker & Hargittai, 2018).

This gap is expected to narrow as the baby boom generation ages (Jesdanun, 2004). Aging baby boomers are expected to rely more on technology for communication and activities of daily living compared to generations before them. However, experts are still not clear as to how the fluency in technology usage during their productive and earlier years will translate into rates of technology adoption (O'Brien et al., 2008).

Socio-economic status (education and income): Although senior citizens in the US are often late in adopting new technologies compared to the younger generations, data from the Pew Research Center show an increase in the rate of adoption of new technologies by those age 65 or older, especially those who are highly educated or affluent (O'Brien et al., 2008; A. Smith, 2014). On the other hand, older adults who are less affluent or have little education and have health or physical disabilities are less likely to keep up with new technology (Hunsaker & Hargittai, 2018).

According to O'Brien et al. (2008), among adults with annual incomes of less than $20,000 only 15% reported ever using the Internet. For older adults with annual incomes between $20,000 and $49,000, the rate increased to 40%. For those with incomes in the excess of $50,000 a year, the rate of internet usage increased to 65%. Older adults with annual incomes greater than $60,000 reported significantly higher usage across technology platforms and activities compared to other income segments. Similarly, older adults' education level greatly influenced their Internet usage. Among older adults with an education level of high school or less, only 18% reported Internet usage, compared to 45% of those with some college education and 60% of those with a college education.

Gender is another variable that has been found to influence not necessarily the level of technology usage, but what older adults use technology like the Internet for (Care-Innovations, 2013; O'Brien et al., 2008). For example, men use the Internet for recreation or entertainment, bill

paying, or stock trading more than women. Women on the other hand use the Internet to explore topics such as health and religion more than their male counterparts.

Family and social structure have also been found to influence the type and extent of technology usage. Research by Intel Corporation found that the size and nature of the social network of friends was a predictor of the type of technology adopted by older adults (O'Brien et al., 2008). This means that older adults tend to adopt the type of technologies used by people they associate with.

Security and privacy concerns: As people age, their concerns about privacy and security increase. Survey results from the Pew Research Center showed that 61% of adults 65 years and older are very uncomfortable about strangers and unsolicited businesses obtaining and sharing personal information about them and their families, compared to 46% of Americans between the ages of 18 and 29 (Care-Innovations, 2013; A. Smith, 2014). These findings suggest that a great deal of care must be taken to ensure that older adults feel at ease using health-related technologies, including a multi-user health kiosk system.

9.0 THE KIOSK PROJECT

Our study was an ancillary investigation to a parent longitudinal study funded by the Agency for Healthcare Research and Quality (AHRQ) being conducted by researchers from the University of Pittsburgh, Carnegie Mellon University, the University of Missouri-Columbia, and the University of Victoria (Canada). The primary purpose of the AHRQ study is to understand factors that influence older adults' use of a multi-user health kiosk as a measurement and intervention delivery system, relative to their needs for a healthier life style.

Multi-user health kiosks were developed to be used for the study. To date, kiosks have been deployed in 10 congregate sites in southwestern Pennsylvania that serve older adults to help them self-manage their health and improve communication with their primary care providers (PCPs). The kiosks enable measurement and transmission of physical and psychological data such as high blood pressure, self-reported symptoms of depression, and other potentially sensitive health information as well as engagement with intervention modules and tracking of users' computer-recognized emotions that prompt adaptive kiosk interaction. All kiosk activities are performed in modular form after the study participant has gone through the initial consent and registration processes for the study. Each participant will have a key fob specifically coded for them and a logon credential (username and password) to be able to access the system.

The kiosk combines traditional telehealth and e-health applications. The telehealth component allows for delivery of healthcare services from a distance. While the e-health component allows for provision of healthcare services through the Internet.

10.0 METHODS

The methodology for this dissertation research had two aims. The first aim explored potential vulnerabilities that existed in a multi-user health kiosk prior to deployment at 10 congregate sites in the Pittsburgh area in Pennsylvania. This allowed us to develop an audit checklist for P&S and confidentiality policies for the kiosk. The second aim explored the efficacy of intervention approaches designed to reduce users' perceptions of risk associated with kiosk use and to increase their intention to use a multi-user health kiosk.

10.1 SPECIFIC AIM 1

Aim 1: Design, implement, and evaluate a new protocol to investigate potential vulnerabilities in a multi-user health kiosk**.**

An exploratory study was performed to detect potential vulnerabilities in the multi-user heath kiosk. To conduct this part of the study, the OCR audit protocol was adapted to create an audit checklist for evaluation of the multi-user health kiosk. Privacy, security and confidentiality policies were then developed for the kiosk based on the evaluation conducted. Finally, a focus group of experts in privacy and security evaluated the P&S and confidentiality policies developed.

10.1.1 Research Question for Aim 1

Do the audit checklist and privacy, security, and confidentiality policies developed for the multi-user health kiosk address the kiosk's P&S and confidentiality issues?

10.1.2 Aim 1 Methods

Preliminary evaluation of the P&S of the multi-user health kiosk was carried out by physically interacting with a prototype of the multi-user health kiosk and by interviewing the programmer who was developing the kiosk software. Based on possible vulnerabilities uncovered from expert opinions in various reviews of literature, interaction with the kiosk, and interviews with the programmer, the OCR audit protocol was adapted to create an audit checklist (Appendix A) for the multi-user health kiosk.

We then used the audit checklist for the multi-user kiosk to develop P&S and confidentiality policies (Appendix B) for our kiosk system. The policies were then incorporated into the design and development process of the multi-user health kiosk. This included the physical kiosk design and logical kiosk design (software and applications) as well as computer systems of the kiosk (networking components).

The P&S and confidentiality policies were incorporated into the physical design of the multi-user health kiosk. This process involved implementing controls to improve the physical parts of the kiosk based on the policies we developed. It also involved making sure unauthorized persons cannot gain physical access to the internal components of the kiosk systems. The design ensured that all hubs, ports (e.g., graphics card, USB, network, serial ports), hard drives, and other internal

components of the kiosk are well enclosed to prevent access by unauthorized users. The new kiosk design included steps to prevent access to network cables, power cables, and other cables employed to attach peripheral devices to the kiosk. This was necessary to prevent individuals from compromising the kiosk system to install computer and network devices as well as rootkit software that could be used to engage in malicious activities on the kiosk and breach kiosk security. Physically securing the kiosk system also helped to guard against the theft of kiosk components such as the hard drive, which is a serious violation of HIPAA/HITECH rules.

The P&S and confidentiality policies were also applied to the design of the kiosk software, computer configuration, and configuration of other hardware components. The policies were also taken into consideration when the kiosk was integrated into the underlying computer network and/or systems.

Finally, the P&S and confidentiality policies were summarized into a privacy statement that explains in language directed to kiosk users the P&S and confidentiality policies implemented in the kiosk system. This privacy statement was used with the minimal intervention and intensive intervention groups involved in the intervention trial that was performed to address part of Aim 2 of this dissertation.

10.1.3 Aim 1 Data Analysis

A gap analysis was performed to determine which of the P&S and confidentiality provisions followed the OCR protocol. A gap analysis is a study which provides information that deals with the current state and the desired future state of an information system. A careful review of the P&S policies was performed by our research team and the programmer developing the kiosk to

determine criteria for implementing items in the security policies developed for the kiosk. The criteria for policy implementation were based on the criticality of items as well as the availability of resources needed to implement those items. Descriptive statistics such as frequencies and percentages were computed based on the results of this gap analysis (Christiansen, 2013). We computed the percentage of 'Yes,' 'No,' and 'N/A' answers on the audit checklist (Appendix A). The results were tallied as shown in Appendix E. This allowed us to quantify the proportions of the P&S and confidentiality policies that have been implemented versus those that still need to be implemented.

10.2 SPECIFIC AIM 2

Aim 2: Test the feasibility and preliminary efficacy of an intervention to reduce users' perceived risk of breaches to P&S and to explore their intention to use a multi-user health kiosk.

10.2.1 Research Questions for Aim 2

Q1: Is it feasible to implement a randomized controlled trial to investigate the preliminary efficacy of an intervention to reduce users' "perceived risk"?

Q2: Does receiving a printed summary of P&S and confidentiality policies implemented in the kiosk, either alone or in combination with a detailed oral explanation of the policies, affect users' "perceived risk"?

$HQ2_0$: Users' "perceived risk" of a health kiosk will not be affected by receiving a print summary or a print summary plus a detailed oral explanation of P&S and confidentiality policies.

$HQ2_1$: Users will have the lowest level of "perceived risk" if they receive a print summary of the P&S and confidentiality policies as well as get a detailed oral explanation of the policies (Intensive intervention group) compared to those who just receive a print copy of the P&S policies (minimal intervention group) and those who receive no intervention beyond the explanation about privacy protections that is part of orientation to the kiosk (control group).

Q3: Is users' "intention to use" the health kiosk associated with their level of "perceived risk"?

$HQ3_0$: Users "perceived risk" will have no correlation to their intention to use the kiosk.

$HQ3_1$: A lower user "perceived risk" will have a positive correlation to "intention to use."

10.2.2 Aim 2 Methods

Adults 21 years of age and older who were participating in the parent study at nine of the congregate sites where the kiosks had been deployed were surveyed during performance assessments conducted at baseline and six months. Participants were required to be community-residing or living in an assisted living environment, able to read and understand English, and able to see and hear well enough (with corrective lenses and/or hearing aids, if necessary) to watch television and view images on a computer screen, listen to the radio, and carry on a phone conversation. Their eligibility had previously been established through prior screening for the Health Kiosk Project, the parent study for which this dissertation constitutes an ancillary study and from which demographic data were provided to describe our sample.

The block or random permuted blocks method was used in the randomization process, in an effort to ensure treatments were balanced for a given block size (Nagin & Weisburd, 2013). Because we had three groups (control [A], minimal intervention [B], and intensive intervention [C]), we had a block size of six (3*2=6). The following example is a depiction of the order in which study participants were intended to be randomized to their respective groups: AABBCC, ABCABC, CABBAC or BACCBA. This meant that after the first block we would ideally have an equal number of participants in each group. To accomplish this, we used an Excel spreadsheet to randomize the letters ABC. We then assigned numbers 1,2,3… to the letters. We wrote these numbers at the back of the envelopes as we stuffed them with the study materials for each group ABC. The envelopes were then sealed to make sure only the study participant could see the content of the envelope that was handed to them. This process ensured that the study was completely blinded so that the person handing the envelopes to the study participants did not know their group assignments. The survey that was administered had a slot for recording the number at the back of every envelope. When we got the surveys back, we matched the envelope numbers recorded on the surveys to our Excel spread sheet to determine which group the participant belonged to in order to administer the right intervention.

At baseline, participants were asked to respond to a paper-based, investigator-developed survey questionnaire on P&S and confidentiality as well as to indicate their intention to use the health kiosk over the next six months. The survey questionnaire was administered prior to completing a battery of performance-based tests of cognition, mobility, and balance for the Health Kiosk Project (Appendix D). The response options to the questions on each questionnaire were ranked and scored as follows: Strongly Disagree -1, Disagree -2, Neither Agree/Disagree -3, Agree -4, and Strongly Agree -5 for the “Perceived Risk” part of the questionnaire and “Yes” or “No”

for the "Intent to Use" part of the questionnaire. The intent to use part also had space for participants to provide a short explanation if they answered "No" on the "Intent to Use" question. After completing the questionnaire, participants were randomly assigned to one of three groups (control, minimal intervention, or intensive intervention) and received the numbered envelope with the study materials for their group assignment. The minimal intervention group received a copy of a summary of the security policies (Appendix C), while the intensive intervention group received a summary of the policies and a phone call to have the policies explained to them. The control group received neither a printed summary nor a phone call to explain the P&S policies to them.

The control group envelope included a printed script that read, *"Thanks for completing the survey. You will be asked to complete another survey when you came back for your six-month review."* The minimal intervention group received a printed script that read, *"Thanks for completing the survey. Please take time to read a summary of the necessary steps that have been taken to protect your information in the kiosk. You will be asked to complete another survey when you came back for your six-month review,"* along with a print copy of the P&S policies for the kiosk. The intensive intervention group was given a printed script that read, *"Thanks for completing the survey. Please take time to read the necessary steps that have been taken to protect your information in the kiosk. A member of the kiosk's project team will be contacting you to schedule a session for detailed explanation of the steps and procedures put in place to make sure your information that you enter at the kiosk is secured. You will be asked to complete another survey when you come back for your six-month review."* The script for the intensive intervention (see Appendix F) was used to explain the items in the P&S statement and to ensure consistency in the information provided during each phone session with each participant in this group. During a one-on-one session for repeated mobility and balance testing at 6 months, participants in all three

groups were asked to respond once again to the same questionnaire that they had completed at baseline.

10.2.3 Aim 2 Sample Size Justification

We expected to recruit 100 participants for our study, with an attrition rate of 40% from baseline to the six-month follow-up period. Hence, we expected to have a total sample size of 60 participants. Because this was a feasibility study and we did not have prior effect size estimates for our outcomes, we calculated a possible range of sample sizes. Calculations represent a given sample size and the detectable effect size (*f*) for a within-between interaction using a two-tailed repeated measures ANOVA with three groups over two time points, with alpha at .05 and power of 80%:

Table 8: Effect Size Estimates Based on Sample Size

TOTAL SAMPLE SIZE	EFFECT SIZE (f)
30	.29
40	.26
50	.23
60	.21

Cohen describes an effect size of $f = .10$ as small, $f = .25$ as moderate and $f = .40$ as large (Coe, 2002). With a sample size of 60 participants, we will have 80% power to detect a small to moderate within-between interaction effect of $f = .21$.

10.2.4 Aim 2 Data Analysis

Q1: Is it feasible to implement a randomized controlled trial to investigate the efficacy of an intervention to explore the magnitude of differences in users' "perceived risk" of P&S breaches as well as correlation between "perceived risk" and their "intention to use" a multi-user health kiosk?

To answer our first research question, we collected information to assess the feasibility of our intervention. Next, we assessed the appropriateness of our randomization process by determining if equal (or near equal) numbers of participants were distributed among the three groups. We also evaluated the feasibility of retaining participants in the study. Our goal was to retain 60% of participants at follow-up.

Q2: Does receiving a printed summary of P&S and confidentiality policies implemented in the kiosk, either alone or in combination with a detailed oral explanation of the policies, affect users' "perceived risk"?

$HQ2_0$: Users' "perceived risk" of a health kiosk will not be affected by receiving a print summary or print summary plus detailed oral explanation of P&S and confidentiality policies.

$HQ2_1$: Users will have the lowest level of "perceived risk" if they receive a print summary of the P&S and confidentiality policies as well as get a detailed oral explanation of the policies (intensive intervention) compared to those who just receive a print copy of the P&S policies (minimal intervention) and those who receive no intervention beyond the explanation about privacy protections that is part of orientation to the kiosk (control).

Our independent variables (IVs) for Question 2 were group (control, minimal intervention group, and intensive intervention) and time (baseline and six-month follow-up). Our dependent variables (DVs) were "Perceived Risk" and "Intention to use."

Perceived risk was measured by taking the average of the scores of user answers to P&S and confidentiality questions. High average/mean scores would correspond to low "perceived risk."

10.2.5 Preliminary Analyses

All statistical analyses were performed using Statistical Packages for the Social Sciences (IBM SPSS, v 25) with a significance level set to.05.

Prior to our primary analysis (repeated measures ANOVA), we tested for the assumptions of normality and compound symmetry. A Shapiro-Wilk test was performed to test for normality of our dependent variables ("perceived risk" and "intention to use") in our three groups (control, minimal intervention, and intensive intervention). The Shapiro-Wilk test p-value should be above.05 for normality. We also visualized the graphs generated by SPSS (histograms, Normal Q-Q plot and box plots) to further cross-check for normality results from the Shapiro-Wilk test (Razali & Wah, 2011). To test for compound symmetry, we used Box's M and Mauchly's test for Sphericity to see if variances of the differences between all combinations of related groups are equal (Keselman, Rogan, Mendoza, & Breen, 1980; R. G. O'Brien & Kaiser, 1985). Both tests should be non-significant for the data to meet the assumption.

An advantage to using a repeated measures ANOVA is that it is considered by most researchers to be robust enough to accommodate issues with non-normal and non-homogenous

data (Fife-Schaw, 2014; Huck, Cormier, & Bounds, 2000). However, if there are severe departures from normality, we planned to switch to an alternative method such as the generalized linear model.

10.2.6 Primary Analysis

We performed 3 X 2 repeated measures ANOVA with a between-subjects factor (group) and a within subject factor (time) for our "perceived risk" DV. The group factor had three levels (control, minimal intervention, and intensive intervention), while the time factor had two levels (baseline and 6 months). For the ANOVA, we examined test statistics with standard errors, 95% confidence intervals, and effect sizes to evaluate for preliminary efficacy of our intervention. Because this was a preliminary study, we were more interested in the magnitude of the effect (effect size) estimates, to be used to power a larger, more confirmatory study.

The table below shows how our 3x2 repeated measures ANOVA was designed. The cells were used to represent the DV ("perceived risk") for the ANOVA that was be performed.

Table 9: 3*2 Repeated Measure ANOVA Table

GROUP	TIME	
	BASELINE	SIX MONTH FOLLOW-UP
CONTROL		
MINIMAL INTERVENTION		
INTENSIVE INTERVENTION		

The primary purpose of the ANOVA was to determine if there was interaction between our two factors (group and time) on our dependent variable ("perceived risk"). In other words, we wanted to find out if the change in kiosk users' "perceived risk" was the result of the interaction between the type of intervention (control, minimal intervention or intense intervention) and time (baseline and six-month follow-up).

The repeated measures ANOVA analysis we performed allowed us to (Huck et al., 2000):

- Evaluate the group-by-time interaction to see if there is a significant difference in "perceived risk "among kiosk users due to interaction between their group (control, minimal intervention, and intensive intervention) and time (base line and six-month follow-up) (group by time interaction effect).

- Evaluate the between-group effect to see if there are significant differences in "perceived risk" between the three groups (main effect of group).

- Evaluate the within-group effect to see if there are significant group differences in "perceived risk over time, from pre (baseline) to post (six months) (main effect of time).

We did not observe any significant difference in "perceived risk" as a result of interaction between the intervention type (control, minimal and intensive intervention) and time (baseline and six-month follow-up), hence we did not perform a simple main effect analysis of group against time. Main effect of group was also not significant. However, we observed a small but significant decrease in "perceived risk "with time. Hence, we did not perform any post-hoc analysis.

Q3: Is users' "intention to use" the health kiosk associated with their level of "perceived risk"?

$HQ3_0$: Users' "perceived risk" will have no correlation to their intention to use the kiosk.

HQ3$_1$: Users' "perceived risk" will have a positive correlation to "intention to use. "

These analyses could not be performed since all the participants answered "Yes" on their intent to use questionnaire at baseline and six-month follow-up (see Appendix H).

Prior to conducting a correlational analysis, we would have tested to see if there was a linear relationship between our two DVs ("perceived risk "and "intention to use"). To accomplish this, we would have plotted our "perceived risk" against our "intention to use" to create a scatter plot. We could then visually examine the scatter plot for linearity as shown in the figure below.

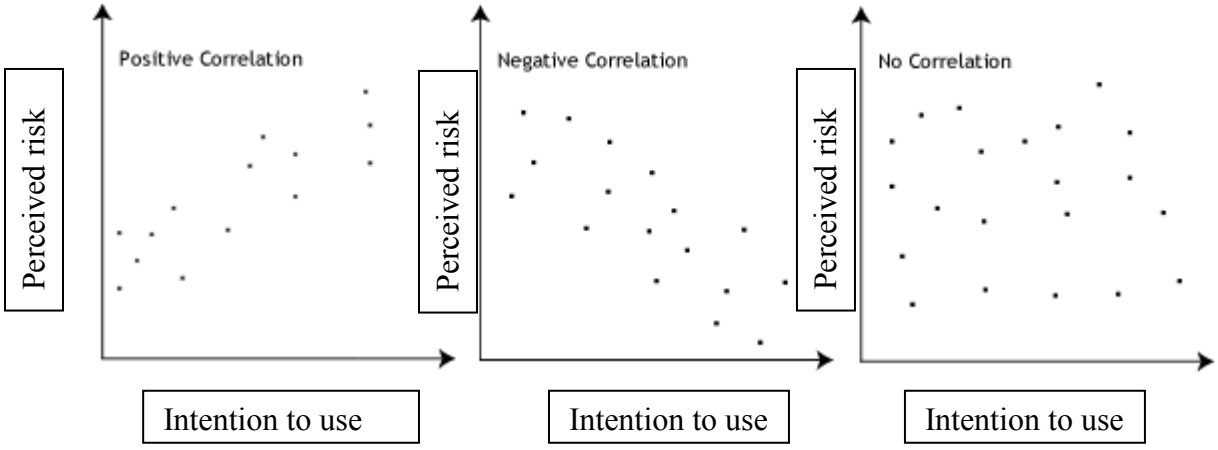

Figure 4: Test for Linearity for Pearson's Correlation

For Pearson's r there should be no significant outliers as it is sensitive to outliers. We would have used "case-wise diagnostics" to detect outliers. Finally, we would have made sure our data are normally distributed. If the data failed the linearity test and normality test, we would have had to switch to Spearman's rank-order correlation. If the assumptions were met, we would have

calculated Pearson's product-moment correlation coefficient to measure the strength and direction of association that exists between "perceived risk" and "intention to use." Pearson's correlation coefficient ranges from r =+1 to r = -1. A correlation coefficient of r = +1 would have meant a perfect positive correlation, while a correlation coefficient of r= -1 would have meant a perfect negative correlation (Huck et al., 2000).

Timeline for data collection

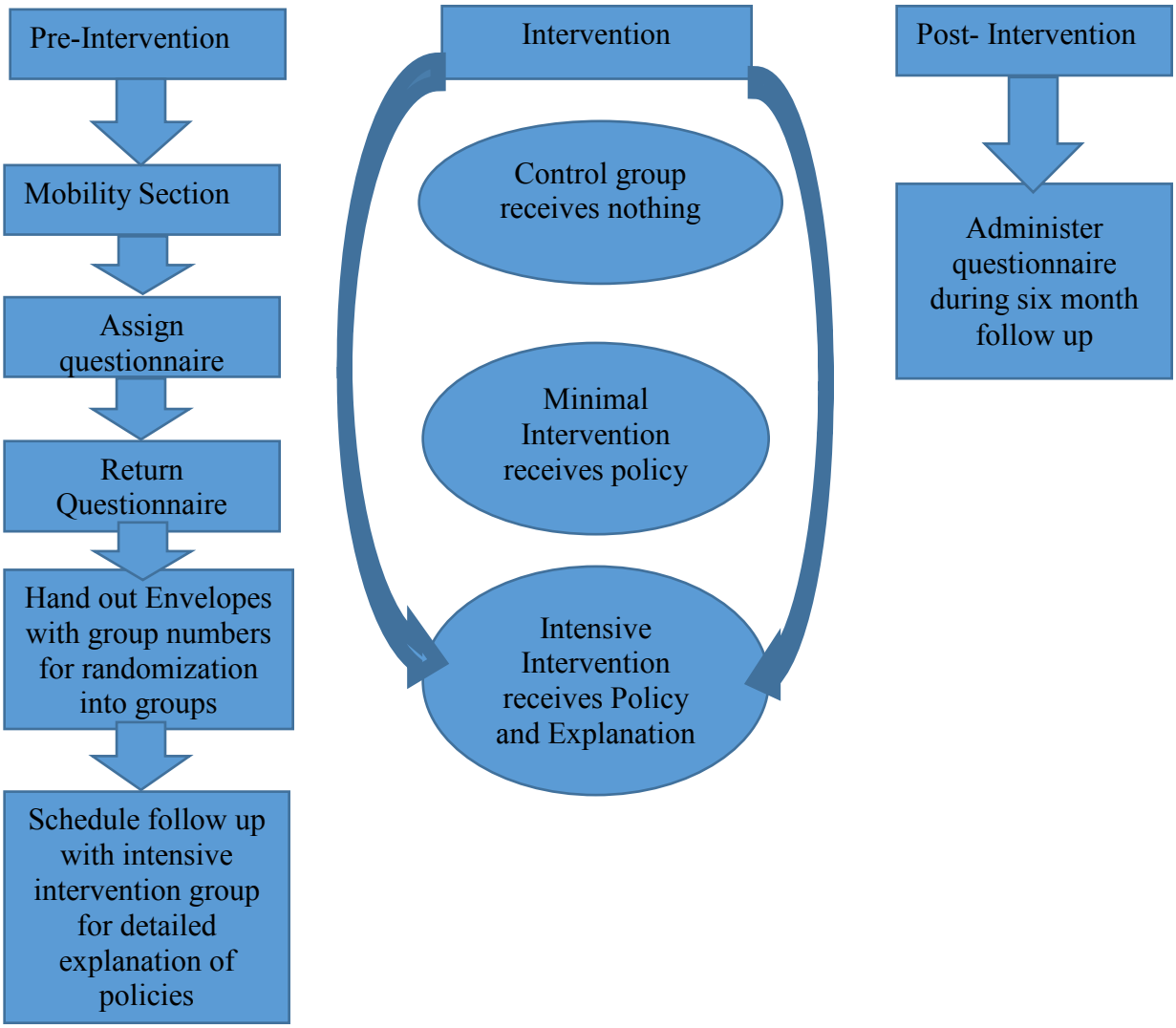

Figure 5: Timeline for data collection

Table 10: Summary of Methods

Hypothesis	Specific Aim	Methods	Data Analysis	Expected Outcome
1. Does the audit checklist and privacy, security, and confidentiality policies developed for the multi-user health kiosk address the kiosk's P&S and confidentiality issues?	1. Design, implement, and evaluate a new privacy and security protocol	1. Exploratory Study Audit Checklist Gap Analysis	1. Descriptive Statistics	1. To investigate potential vulnerabilities in a multi-user health kiosk. Implement 50% of what is found on gap analysis
2. Users' "perceived risk" of a health kiosk will not be affected by receiving a print summary or print summary plus detailed oral explanation of P&S and confidentiality policies.	2. Test the feasibility and preliminary efficacy of an intervention to reduce users' perceived risk and to explore their intention to use a multi-user health kiosk.	2. Randomized control study with three groups (control group, minimal intervention group, and intensive intervention group	2. 3X2 repeated measure ANOVA Spearman's Correlation Coefficient	2. To see if user "perceived risk" will decrease if they read a summary of the security policies To see if there is a correlation between users "perceived risk" and "intention to use"

10.2.7 Missing Values /Drop out

Because our study was a pre-post-test study, there was a good chance that some of the participants would drop out before the six-month follow-up appointment. There was also a likelihood of some participants not completing the intervention. Thus, we used complete case data for the analysis.

Only 36 participants had both baseline and six-month follow-up data when we suspended data collection to perform data analysis for this dissertation. Seventy-four of the participants did not have six-month follow-up data. Thirty-seven participants out of the 74 were not due for their six-month follow-up and 37 were due for their six-month follow-up. Of the 37 who were due for their six-month follow-up, 11 dropped out due to personal reasons (sickness, busy, moved, family emergency, etc.), 16 had no six-month follow-up data for unexplained reasons, 9 were erroneously not handed a six-month P&S survey, and one participant could not be reached (see Table 11).

Table 11: Sample break down (N=110)

Category	Number of participants
Both baseline and six-month data	36
Unreachable	1
Not due for six-month follow-up	37
Dropped out	11
No six-month follow-up data	16
No P&S survey handed out by error	9

11.0 DEMOGRAPHICS/SAMPLE CHARACTERISTICS

We were able to randomize 110 participants into our sample at baseline. Only 36 (32.7%) of them made it to the six-month follow-up and 74 (67.3%) had only baseline data at the time of our data analysis. Table 12 shows comparison of the 36 participants with both baseline and six-month data and the 74 participants with only baseline data. We performed an independent t-Test for the continuous variables and $\chi 2$ for categorical variables.

Table 12: Comparison of participants with both baseline data and six-month follow-up data and those with only baseline data (N = 110)

Variable	Baseline and Six-month follow-up data	Baseline data only	P	Statistic
Age M(SD)	72.69(7.18)	74.39(8.74) _	.32	$t_{108} = 1.71$
Gender n (%)				
Female	29(26.36%)	61(55.45%)	.81	$\chi^2_1 = .06$
Male	7 (6.37%)	13(11.82%)		
Income n (%)				
Low income <$40,000	21(19.09%)	35(31.82%)	.13	$\chi^2_1 = 2.3$
High income ≥ $40,000	10(9.09%)	33(30.00%)		
Missing	5(4.54%)	6(5.46%)		
Eyesight n (%)				
Poor- Fair	9 (8.18 %)	21(19.09%)	.84	$\chi^2_1 = .042$
Good	25(22.73%)	53(48.18%)		
Missing	2(1.82%)	0(0%)		
Hearing n (%)				
Poor-Fair	9(8.18%)	18(16.36%)	.71	$\chi^2_1 = .14$
Good	23(20.91%)	55(50.00%)		
Missing	4(3.64%)	1(.91%)		

Table 12 (continued)

In general, to what extent do you believe technology reduces privacy M(SD)	7.34(2.10)	6.68(2.71)	.21	$t_{106} = 4.31$

We performed the analysis for findings shown in Table 12 to be sure that nothing in the methodology of the study design caused 74 of the participants to not complete the six-month follow-up. All the *P* values were greater than .05 hence there were no significant differences between the 36 participants with both baseline and six-month follow-up data and the 74 with only baseline data that made them not make it to the six-month follow-up.

Table 13 shows the sample characteristics of the 36 participants that were included in the analysis. We performed a One-way ANOVA for the continuous variables and $\chi 2$ test for the categorical variables.

Table 13: Comparison of selected characteristics, by group (N = 36)

Variable	Control	Minimal	Intensive	P	Statistic
Gender n (%)					
Female	11(30.55%)	9(25%)	9(25%)	.66	$\chi_1^2 = .84$
Male	3(8.33%)	3(8.33%)	1(2.79%)		

Table 13 (continued)

Income					
Low income<$40,000	10(27.79%)	7(19.44%)	4(11.11%)	.62	$\chi^2_1 = .94$
High income ≥ $40,000	3(8.33%)	4(11.11%)	3(8.33%)		
Missing	1(2.78%)	1(2.78%)	3(8.33%)		
Eyesight N (%)					
Poor- Fair	4(11.11%)	3(8.33%)	2(5.56%)	.94	$\chi^2_1 = .92$
Good	10(27.78%)	8(22.22%)	7(19.44)		
Missing	0(0%)	1(2.78%)	1(2.78%)		
Hearing N (%)					
Poor-Fair	3(8.33%)	4(11.11%)	2(5.56%)	.28	$\chi^2_1 = 2.53$
Good	11(30.56%)	4(11.11%)	8(22.22%)		
Missing	0(0%)	4(11.11%)	0(0%)		
Age F(n^2)	$F(2,35) = .05$, $n^2 = 5.3$			.95	
In general, to what extent do you believe technology reduces privacy F(n^2)	$F(2,34)=.34$, $n^2 = 3.15$			.71	

This analysis in Table 12 was performed to test if our randomization procedure worked and whether the randomization still held true for the 36 participants that we used in our 3*2 repeated measures ANOVA. All our *P* values were greater than .05 (not significant), hence our randomization procedure still held true in the three groups that made up the 36 participants that were included in our final analysis.

Table 14 summarizes the demographic information of the 36 study participants with both the baseline and six-month follow-up questionnaire data. Twenty-nine (80.56 %) were female and 7 (19.44 %) were male. Twelve (33.34 %) of the participants were 60-69 years old, 17 (47.22%) were 70-79 years old and 7 (19.44%) were 80+ years old. For education level, 11 (30.55%) completed high school, 10 (27.78%) had some college education and 14 (38.89%) completed a college education. Two (5.55%) never used a computer before, 13 (36.11%) considered their computer skill as beginners, and 20 (55.56%) said they were competent computer users. Twenty-one (58.33%) had low income<$40,000, 10(27.78%) reported high incomes>$40,000 and 5 (13.89%) were not certain how much they made. All 36 participants said English was their primary language. Nine (25.00%) said they had poor-fair eyesight, 25 (69.44%) had good eyesight. For hearing, 9 (25%) had poor-fair hearing, 23 (63.89%), had good hearing.

Table 14: Sample Demographics (N=36)

Characteristic	Subject(n)	Proportion %
Gender		
Male	7	19.44
Female	29	80.56
Age		
60-69	12	33.34
70-79	17	47.22
80+	7	19.44
Education		
High School	11	30.55
Some College	10	27.78
College	14	38.89
Missing	1	2.78
Computer skills		
Never	2	5.55
Beginner	13	36.11
Competent	20	55.56
Missing	1	2.78
Income		
Low income<$40,000	21	58.33
High income ≥ $40,000	0	
Not certain		27.78
	5	
		13.89
English Language	36	100
Eyesight		
Poor- Fair	9	25.00
Good	25	69.44
Missing	2	5.55
Hearing		
Poor-Fair	9	25.00
Good	23	63.89
Missing	4	11.11

12.0 RESULTS

12.1 AIM 1 GAP ANALYSIS RESULTS

Figure 6 shows the results of the gap analysis performed for Aim 1. Our initial goal was to implement those items deemed most critical. Those items were addressed first and foremost and then as time and resources permitted, all other items were addressed. Our aim was to implement 50% of the items referenced on our P&S policies in this version of the kiosk.

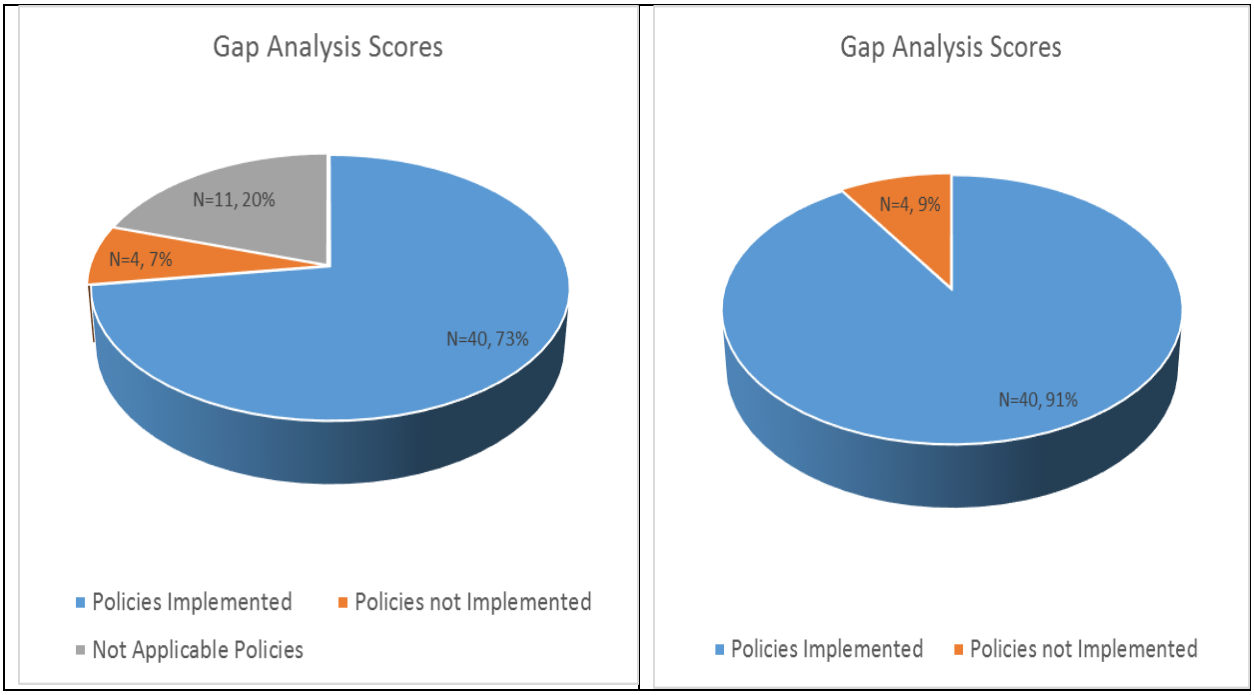

Figure 6: Gap Analysis Results

As shown in figure 6 we were able to implement 73% of our P&S policies as part of our System Development Life Cycle (SDLC) for the current multiuser health kiosk. Seven percent of the policies were not implemented in this version of the kiosk. We also found 20% of our P&S policies from our audit checklist were not applicable to the current release of our kiosk platform. When we filtered out the non-applicable policies, the implementation rate for our P&S policies went up to 91% and the percentage of policies not implemented went up to 9%. This means we surpassed our goal of implementing 50% of applicable P&S policies.

The four (9%) policies that were not implemented are:

- Is there a clear written procedure to grant access to e-PHI?
- Is there any HIPAA and HITECH security awareness and training program in place?
- Are there any policies for testing emergency contingency plans or backup procedures?
- Are there procedures for terminating access when it is no longer needed?

The Health Kiosk Project is ongoing and so those policies that were not implemented will be addressed.

12.2 AIM2 DATA ANALYSIS RESULTS

12.2.1 Result for Aim 2 Question 1

Our study has shown that it is possible to perform a single-blinded randomized controlled study to investigate the efficacy of an intervention to explore the magnitude of differences in users' "perceived risk" of P&S breaches as well as the correlation between "perceived risk" and their "intention to use" a multi-user health kiosk. However, we did not meet our goal of retaining 60 participants at six-month follow-up.

12.2.2 Descriptive Statistics

Analysis was performed on 36 participants and results are shown in Table 15. The control group (1) had 14 participants with a pre-perceived-risk mean and standard deviation of 3.90 and .82, respectively, and a post-perceived-risk mean and standard deviation of 4.20 and .74, respectively. The minimal intervention group (2) had 12 participants with pre-perceived-risk mean and standard deviation of 3.99 and .52 respectively, and a post-perceived-risk mean and standard deviation of 4.38 and .55 respectively. The intensive intervention group had 10 participants with a pre-perceived-risk mean and standard deviation of 4.32 and .52 respectively, and a post-perceived-risk mean and standard deviation of 4.47 and .59, respectively.

Table 15: Descriptive Statistics of Perceived Risk, by Group (N = 36)

Descriptive Statistics

	Group ID	Mean	Std. Deviation	N
Pre-Perceived-Risk	1	3.90178571	.815286501	14
	2	3.98958333	.523478133	12
	3	4.32336957	.521176373	10
	Total	4.04815821	.658970562	36
Post-Perceived-Risk	1	4.20238095	.741197839	14
	2	4.37552838	.554587337	12
	3	4.47277778	.594948730	10
	Total	4.33520699	.636206274	36

1= strongly disagree – 5 = strongly agree; higher the number the less perceived risk
Group 1=Control Group(A), Group 2= Minimal Intervention Group (B) Group 3= Intensive Intervention Group (C)

12.2.3 Assumptions for Aim 2 Question 2 (3 X 2 repeated measures ANOVA)

Box's M test for compound symmetry was not significant. Hence, the compound symmetry assumption was met. Mauchly's test for sphericity was non-conclusive since we only had 2 levels of our DV (Perceived Risk). Apart from the control group at baseline, all other group/time combinations were normal. Even though the control did not meet the assumption for normality at base line, ANOVA is robust to the normality assumption.

12.2.4 Results of 3*2 Repeated Measures ANOVA

The results from the 3*2 repeated measures ANOVA showed no significant group-by-time interaction (no Time*Group interaction) F (2, 33) = .27 P=.77, ηp2=.02. This means there was no significant change in perceived risk among kiosk users due to interaction between their group (control group [A or 1], minimal intervention group [B or 2] and intensive intervention group [C or 3]) and time (baseline and six-month follow-up). There was a significant main effect of time F (1, 33) = 4.73, P=.04, ηp2=.13. Hence, there were significant differences in perceived risk over time regardless of group. Also, there were no significant differences in perceived risk between the

three groups (control, minimal intervention and intensive intervention) F (2, 33) =1.27, P=.30 ηp2=.07 (no main effect of group) (see Table 16).

Table 16: Main Effect of Group, Time and Interaction results of Time* Group (N = 36)

Source	SS	df	MS	*F*	*p*	ηp2
Between-Subjects Effects	18.24	33	.55			
GroupID	1.40	2	.70	1.27	.30	.07
Within-Subjects Effects	9.57	33	.29			
Time	1.37	1	1.37	4.73	.04	.13
Time * GroupID	.16	2	.077	.267	.77	.02

As shown in Figure 7, perceived risk decreased across all the three groups with time (higher values correspond to lower perceived risk). The intensive intervention group had the lowest perceived risk in the six-month follow-up, followed by the minimal intervention group and the control group.

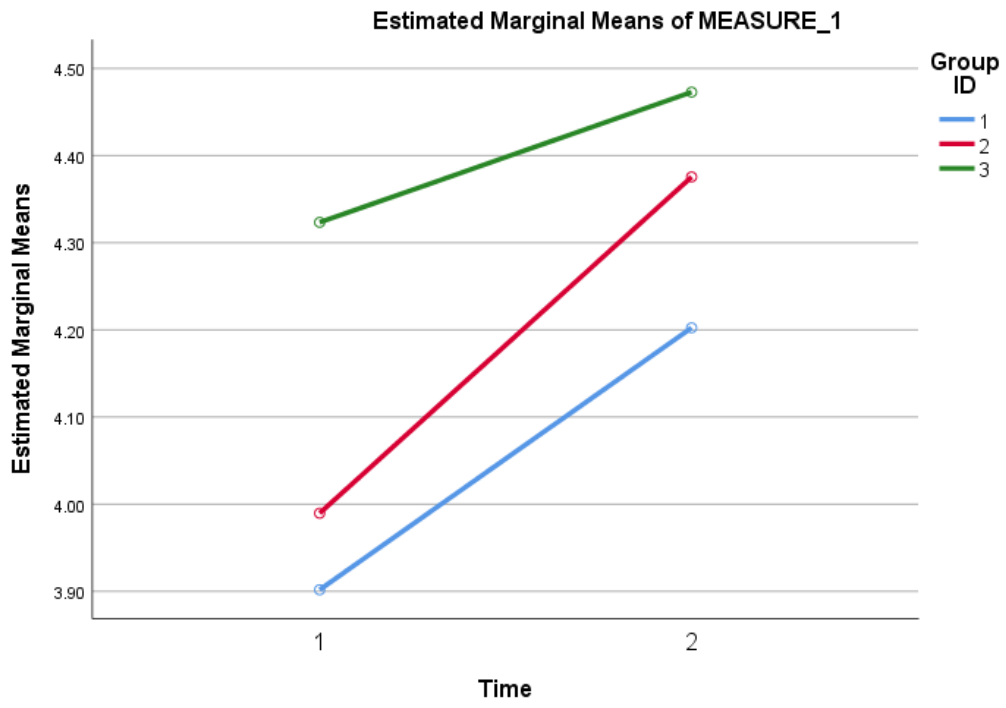

Figure 7: Plot of Estimated Marginal Means

Group 1=Control Group(A), Group 2= Minimal Intervention Group (B) Group 3= Intensive Intervention Group (C) (Higher values corresponds to lower perceived risk)

13.0 DISCUSSIONS

13.1 AIM 1 GAP ANALYSIS DISCUSSIONS

A 2015 study on the implementation of IT P&S policies in the retail sector in South Africa concluded that there was a significant lack of IT P&S policies, processes, procedures and corresponding documentation (van Vuuren, Kritzinger, & Mueller, 2015). A summary of the results is shown in Table 17.

Table 17: GAP in IS P&S policies

GAP in IS Policies, Processes and Procedures And actual Implementation		
Percentage not implemented	Findings	Percentage implanted
55%	Not informed of Applicable work-related information systems (IS) P&S Policies when they joined the company.	45%
62%	Employees did not sign any document to show that they were provided P&S policies highlighting their responsibilities towards protecting organization IS assets.	38%
96%	Employees said that there was no documentation of IS P&S polices or did not know of existence of documentation of steps (instructions/procedures) to follow to implement controls required for their work environment.	4%

Table 17 (continued)

91%	Employees state that they did not receive training or updated company IS P&S policies in the past year	9%
39%	Employees were not aware of enforcement of new company IS P&S policies or are not informed about those policies. Of the 61whos said they were made aware of the polices, only 5% went through periodic training programs, 30% were informed through the grape vine and 65% via email or other ad-hoc means.	61%
68.6%	Average	31.4%

Their reporting showed an average 31.4% implementation/enforcement of IT P&S policies, processes, procedures and corresponding documentation. Other studies have strongly linked the GAP in IT P&S policies and actual implementation/enforcement of the P&S policies to the recent increase in breaches (Kafali et al., 2017). A recent HIPAA case study which looked at 1577 breaches reported by Health and Human Services (HHS) found gaps between HIPAA and reported breaches, that led to a coverage/enforcement rate of 65% (Kafali et al., 2017). This means actual polices implementation is 65% of what is supposed to be implemented. Hence, our implementation rate was much higher compared to what has previously been reported. This also means that overall our multi-user kiosk design is quite secure compare to other systems. The policies that we did not implement (9% of policies not implemented) were the ones that needed an addendum to make them complete. For example, we have a policy which states that all access to the kiosk and its resources must be terminated once a kiosk project member is no longer with the kiosk project. However, there was no detailed written procedure yet for terminating access to the kiosk. The GAP

analysis results are supposed to help us improve our P&S policies. Hence, like other studies, we should have categorized our GAP analysis into the various sections of our P&S policies (Privacy, Confidentiality, Security, etc.) because this would have allowed us to view which categories of the P&S policies needed more work or improvement (Mineraud, Mazhelis, Su, & Tarkoma, 2016).

13.2 AIM2 QUESTION 1 DISCUSSION

We were able to show that it is possible to perform a single-blinded, randomized, controlled study to investigate the efficacy of an intervention to explore the magnitude of differences in users' "perceived risk" of P&S breaches as well as the correlation between "perceived risk" and their "intention to use" a multi-user health kiosk. One thing we uncovered right at the beginning of the study was that we needed to tweak our randomization procedure to make the data collector blinded to the participant's group assignment. Initially, we were putting the group IDs (A, B, C) directly on the envelope labels. That meant that the person handing the envelopes containing the survey questionnaire would have known to which group the participant was being randomized. We therefore created a "master Excel sheet" (Appendix G) of numbers that matched the group IDs (A, B, C). We put those numbers on the back of the envelopes and the participant ID at the top of each survey questionnaire. Once completed, each survey questionnaire administered at six months was paired with its baseline counterpart.

13.3 AIM 2 QUESTION 2 DISCUSSION

Our study was consistent with characteristics of most feasibility studies. Feasibility studies are usually used to test ideas (study design, practicality, sample-size, randomization procedure, data analysis type, etc.) for a more extensive, full-scale or future study (Bowen et al., 2009). In general, there are eight areas of focus in feasibility studies (Bowen et al., 2009):

Acceptability looks at how both the targeted individuals and those administering the programs react to the intervention. For example, did the kiosk study coordinators follow the study script correctly and did the kiosk study participants understand or follow the intervention instructions correctly?

Demand involves gathering data by documenting the actual use of the intervention activities in a defined population or setting to evaluate the intervention. For our kiosk project we used a questionnaire to collect data from the participants and an Excel spreadsheet to input our data. In the future, we will add a date field to the questionnaire to ensure capture of the date the questionnaire was administered, and we will add a date field to our Excel spreadsheet to record the date. This will allow us to easily keep track of when a participant first completed a baseline survey and received his or her group assignment, furthering allow us to know when a participant missed their six-month follow-up, so we can contact them.

Implementation is usually done in an uncontrolled process or design, and is the extent, likelihood, and manner in which an intervention can be fully implemented as planned and proposed. Our study was controlled, and it was a Single Blinded Randomized Control Trial.

Practicality focuses on the extent to which the intervention can be delivered within constraints of time, resources, commitment, sample population, etc. We were constrained by time

because this was a dissertation and therefore had to completed within a set period. Another constraint was that we ended up deploying in 10 locations instead of the initial one location. Hence, we decided to perform the intensive intervention follow-up to explain P&S policies by phone.

Adaptation is making the appropriate changes to procedures and program content to accommodate requirements of a different media or population. Explanation of P&S polices were done on the phone instead of face-to-face. We also had to tweak our randomization procedure to make sure the study was single blinded so that the data collector remained unaware of the participant's group assignment.

Integration focuses on changes that need to be put in place to integrate a new program, process or design into an existing one. We had to integrate the procedures for our study into those established by the parent study.

Expansion deals with the possibility of expanding an already successful intervention with a different population or different setting. This did not pertain to our study.

Limited-efficacy testing, most feasibility studies involve limited testing of an intervention. This could be done with a sample of convenience, preliminary data, intermediate rather than final outcomes, shorter follow-up periods, or limited statistical power. Our study was ancillary to another study and, hence, we had to use a sample of convenience. We also used intermediate data since we are still collecting data.

We did not meet our goal of retaining 60 participants in our study at the sixth-month follow-up. This was due in part to the fact that we did not deploy all the 10 kiosks at the same time. Hence, some the participants were not due for their six-month follow-up at the time of our data analysis. This is consistent with "practicality" explanation of feasibility studies (Bowen et al.,

2009). We had to suspend our data collection to run a preliminary analysis for the dissertation. We therefore, had a small sample of 36 for our data analysis. The small sample size can affect the power of our study as well as reduce the potential of arriving at statistically significant outcomes (Faber & Fonseca, 2014). This may explain why we did not observe significance in the main effect for group or in a time*group interaction. In the future we will recruit more people into the study to improve the chances of having more than 36 people after six-months. Other studies have shown that intensive follow-up contact with subjects seems to improve continuous participation in research studies and retention of participants (Yancey, Ortega, & Kumanyika, 2006). Hence, we will have to find a way to have a more intensive follow-up without coming across as harassing our study participants. All this fits into the "limited efficacy testing" of feasibility studies (Bowen et al., 2009).

Trust has been found to be one of the major determinants of "perceived risk". High trust correlates to low "perceived risk" (Fox & Connolly, 2018; van Schaik et al., 2017). Participants in All three or our groups had a very low (saturated) "perceived risk" at baseline. This may have been due to participants at the outset having had a very high-level trust in the system and the study they were signing up for. They had only recently consented to take part in the study, so they likely knew/felt or perceived/trusted their information to be safe. They also received a Brief explanation of P&S of the kiosk as part of their orientation to the parent study.

"Perceived risk" decreased with time. This is consistent with previous research which has shown that trust tends to increase with time, and "perceived risk" decreaseS with time as trust increases (Fox & Connolly, 2018).

Studies have shown that people are willing to trade the P&S of their information for very little reward (Kokolakis, 2017). So perhaps for our study participants, sacrificing their P&S to further

research was a good thing to do (this was more rewarding to them). This could be another reason for the low level of "perceived risk" among our three study groups at baseline, as they were willing to sacrifice their P&S to advance research. The low (saturated low level) "perceived risk" meant there was very little room for improvement in response to our intervention. This could be why the magnitude of change in our "perceived risk" with time (main effect of time) was small and no significant changes were detected for a group by time interaction (main effect of group by time) as well as group (main effect of group).

Another explanation for the low-level of "perceived risk " at baseline could be due to what has been described by researchers as the information security and "privacy paradox," characterized by inconsistencies between privacy attitude and privacy behavior (Kokolakis, 2017; Schmidt, 2018). In one study, subjects were asked to buy a DVD from one of two competing stores. One of the stores asked buyers to provide very private and sensitive personal information but offered a small discount on the purchase. The second shop did not ask for private or sensitive personal information from buyers and offered no discounts. Almost all participants were reported to have bought from the cheaper store. The irony was that 75% of the participants said they had a very strong interest in data protection and 95% indicated they had a strong desire to protect their personal information (Kokolakis, 2017). In another study of users' attitude towards P&S, 95% of the participants said they were concerned about their privacy online. However, only 31% said they understood how their personal information was collected and shared. Thirty three percent said they could access the online privacy policies, although only 16% had actually read them. Just 43% said they knew how to change their security setting on social media, but only 29% had actually changed it (see Table 18) (Schmidt, 2018).

Researchers are baffled as to what is causing the dichotomy in user attitude and actual behavior towards privacy and security (P&S). Hence, to improve this study in the future, we will also research cognitive behavior as it relates to P&S to help us in our questionnaire design.

Table 18: User P&S Attitude

User Attitude Towards P&S

Percentage	*Findings*
95%	Of the participants said they were concerned about their privacy online
31%	Only 31% said they understood how their personal information was collected and shared (Why will they not find out if they were that concerned)
33%	Can access the online privacy policies but only 16% read them
43%	knew how, and could change their security setting on social media, but only 29% changed them

The fact that there was a slight reduction in "perceived risk" over six months may be attributable in part to the good work done by the Health Kiosk Project team in designing the kiosk; building its physical structure and the underlying software and computer hardware; incorporating the P&S policies into the kiosk. As was shown in the gap analysis we successfully implemented 91% of our P&S policies. This is very high compared to the industry standards and as reported in other studies(Kafali et al., 2017). This could mean that the participants were very comfortable/trusted using the kiosk from the P&S standpoint. The study coordinators also did a good job to make the study participants comfortable and trusting throughout the duration of the study. The reduction in perceived risk with time (main effect of time) also meant that the users'

trust in our multi-user health kiosk increased with time as they used the kiosk, consistent with findings in the study conducted by Fox and Connolly (Fox & Connolly, 2018).

Questionnaire design is another thing we will have to look at in our future studies. Studies have shown that it is very difficult to design questionnaires that are easy to understand (Krosnick, 2018). Our future questionnaires will be designed in collaboration with the School of Psychology and Education. This collaboration will also involve designing P&S polices and checklists for various information systems.

We were not able to run the correlation analysis for the study. This was because all the study participants answered "Yes" to the intention to use question. In future studies the intention to use question will be designed using a Likert-type scale instead. Compared to "Yes/No" type of question, Likert-type scale questions have the advantage of being very flexible. They provide the ability to measure broad areas or look at specific facets of what the investigator is trying to measure (DV) (Canada, 2018). They are also more precise than "Yes/No" or "True/False" questions, easy to compile and understand (Canada, 2018).

14.0 LIMITATIONS OF OUR STUDY

Our study included adults 60 years of age and older, so it is not generalizable to an entire population. Lack of generalizability affects external validity of our research. Hence, future research will try to recruit participants 21 years and older in order to improve external validity (Schofield, 2002). Because this was an ancillary study to another study, the study participants came in at a "saturated" low-level of "perceived risk," perhaps due to self-selection and due to receiving brief information about P&S measures incorporated into the kiosk design prior to being recruited into our study and receiving the P&S questionnaire. Hence, there was very little room for improvement (Levin, 2005) in this convenience sample, which makes control of extraneous variables difficult (Bowen et al., 2009). In the future participants will be recruited solely for our P&S study to lower the crossover effect from the parent study to which they consented (Levin, 2005). Because this was a feasibility/pilot study, we did not include covariates such as age, socioeconomic variables, gender, etc. in the analysis, so there is no way of telling how much these confounding variables may have affected "perceived risk" to breach of P&S of the multi-user health kiosk. Not accounting for the confounding variables could affect the internal validity of our study (Pourhoseingholi, Baghestani, & Vahedi, 2012). Our plan is to add potentially confounding variables to our future data analysis to allow us to see how those variables affected our intervention (Levin, 2005). We had a small sample of 36 participants at the six-month follow-up. The small sample size could explain for the reason why we did not have significant results (Faber & Fonseca, 2014). Our aim is to recruit more people to our study to improve the sample size. All 36 used in the data analysis answered "Yes" (see Appendix H) regarding their intention to use the kiosk both

at baseline and six-month follow-up so we could not run our correlation analysis. In the future, we will use a Likert-type scale in our "intention to use" questionnaire to capture more responses that could have enabled us to run the correlation analysis (Canada, 2018).

15.0 FUTURE STUDIES

The immediate follow-up with this dissertation is to continue with the data collection for the study to get a larger sample to analyze. A larger sample size might permit detection of significance for a group*time interaction as well as a main effect for group (Faber & Fonseca, 2014). With a larger sample size our analysis will be expanded to include confounding variables like age, gender, income, education and computer skills to see how those affect "perceived risk". Adding potentially confounding variables to our analysis will reduce the possibility of Type I error and improve internal validity of the study (Pourhoseingholi et al., 2012).

Armed with the experience and findings from this study, we will design a future study to see if having a well-designed training for internal users could improve their attitude and positively influence their behavior items of P&S to engage in safe P&S behavior. This will be performed in collaboration with the School of Education and Psychology Department. This is very important since most research has identified the internal user as the source of most of the recent breaches.

Another adventurous and interesting study will be a multi-disciplinary, longitudinal study to create a chronology of all the recent high profile privacy and security breaches and team up with researchers at the School of Education and Psychology Department to see if it is possible to create a profile of those attacks so we can build that profile into machine learning software to help forecast activities leading to a breach. This way we can always be one step ahead of will be attackers.

16.0 CONCLUSION

We were able to research possible vulnerabilities that could pose security risks to multi-user health kiosks. The possible risks were then used to successfully select aspects of the OCR audit protocol to develop an audit checklist for our kiosk. P&S policies were developed successfully from the audit checklist to make sure our P&S policies matched our audit checklist. The P&S policies were then successfully incorporated into our kiosk design (as part of our kiosk SDLC) to make our kiosk secure and compliant with HIPAA/HITECH standards. We were also able to successfully implement 91% of our P&S policies, surpassing the goal of 50% that we had set for this version of our kiosk, as was shown in our gap analysis results. Our P&S implementation rate was also much higher than what has been reported in other studies in the industry 31.4% in one study (van Vuuren et al., 2015) and 65% in another study (Kafali et al., 2017).

We were able to design a single blinded randomized control trial (RCT) and run a pilot study to test the efficacy of an intervention to lower "perceived risk." To our knowledge no one has done RCT studies on P&S. Even though we did not see significant changes due to group*time interaction as well as group, we observed a reduction in "perceived risk" because of main effect of time. A larger sample size could have led to significant results for time*group interaction as well as group. This finding suggests that educating users about the content of the P&S policies of the systems they are using could help to improve attitudes towards P&S and positively influence P&S behavior (van Schaik et al., 2017).

Research has also shown there is general lack of funding in P&S because it is difficult to quantify the momentary gain in information/data security. However, with the recent increase in

high profile breaches, P&S has become one of the main determinants of technology acceptance and adoption (Mitzner et al., 2017) and fines for breaches are on the rise. Hence, organizations will lose out of patronage from users and potentially lose money in the process. Technology development and deployments might fail outright if P&S is not incorporated as part of the systems development cycle. This is evident with the recent complete shutdown or discontinuation of Google+ (Carman, 2018). Fines for information breaches have also increased tremendously. Hence P&S will have to take "a front row seat" in technology development.

More research is needed to find out if a larger sample size could yield more robust results in our pilot study. This study design could also be adapted for research in P&S during systems design and implementation. For instance, it could be adapted to test whether a specific training program or communication of P&S policies could lead to better adherence to P&S polices by both internal and external users. Our findings could serve as a framework to drive policy in P&S of health applications, technology and health IT systems.

APPENDIX A: MULTI-USER HEALTH KIOSK AUDIT CHECKLIST

The protocol below provides a guideline that can be used to assess whether a multi-user health kiosk is meeting P&S regulations such as HIPAA and HITECH. It has been adapted from the OCR audit protocol.(V. J. Watzlaf et al., 2010)

HIPAA/HITECH Compliance Checklist for Multi-User Health Kiosk			
PRIVACY	Yes	NO	N/A
1. Personal Information			
• Is there a privacy policy?			
• Does the kiosk have a privacy screen?			
• Will user information be shared with third-party companies?			
○ If yes, is there a Business Associate (BA) agreement with this company?			
2. Retention of Personal Information			
• Is user information and e-PHI stored?			
• Is there a policy outlining the retention period of e-PHI?			
• Can users request copies of their Information?			
○ If yes, is there a well-defined procedure for requesting copies of PHI and other information?			
CONFIDENTIALITY			
3. Request of Information			
• Is there a policy for disclosure of e-PHI or identifiable information?			

SECURITY			
4. Security Management Process			
• Is there a well-written procedure or protocol for performing a thorough risk assessment?			
• How many times in a year is a risk assessment performed? o 0 times in a year? o Once a year? o Twice a year? o Three times a year? o More than three times a year?			
• Is there a formal or informal policy or procedure to review information system activities like audit logs, access reports incident tracking etc.?			
• Are current security measures sufficient to reduce risk and vulnerabilities to a reasonable level?			
5. Assigned Security Responsibility			
• Do you have a security officer in charge of developing, implementing, monitoring and communicating HIPAA/HITECH security policies and procedures?			
6. Workforce Security			
• Do you have documentation for authorization and supervision of all entities working with or helping to manage and maintain the kiosk?			
• Do you have clear job descriptions for all entities working with the kiosk?			
• Is there documentation listing the level of access to the system, including e-PHI for each employee?			
• Is there a clear procedure to terminate access to resources once a person is removed from the project or terminated?			
7. Information Access Management			
• Is there a clear written procedure to grant access to e-PHI?			
• Do policies and standards exist to authorize and document access, review and modify a user's right to computer systems, software, databases and other network resources?			
• Are users going to pay to use the kiosk system?			

○ If so, will a clearinghouse or third party be used to process payment? ▪ If so, are there policies and procedures for access to information, by clearinghouse workers, consistent with HIPAA and HITECH security rules?			
• Are formal or informal policies and procedures in place for security measures relating to access control?			
• Is there any HIPAA and HITECH security awareness and training program in place?			
• Are there procedures and measures in place for protection from malicious software and exploitation of vulnerabilities?			
• Have employees been trained as to the importance of protecting against malicious software and how to guard against it?			
• Are there policies and procedures for log–on monitoring and password management?			
• Do security training materials target current IT security topics relevant to kiosk security?			
• How often are security procedures, policies and protocols updated? ○ 0 times in a year? ○ Once a year? ○ Twice a year? ○ Three times a year? ○ More than three times a year?			
• Are there any policies and procedures in place to identify, respond to, report and mitigate security incidents?			
8. Contingency Plan			
• Is there a contingency plan in place to identify critical applications, data and other operations of the kiosk system?			
• Is there a disaster recovery and backup plan in place to restore lost data?			
• Is any redundancy built into the kiosk deployment?			
• Is there any well-defined policy for operating in emergency mode that allows continuation of critical business processes?			
• Are there any policies for testing emergency contingency plans or backup procedures?			

9. Evaluation			
• Are there policies in place for evaluating the security procedures as they apply to HIPAA/HITECH security rules?			
10. Business Associate (BA) Contracts			
• Is there a policy for contracts with Business Associates and other third-party vendors?			
11. Physical Security			
• Are there policies in place to analyze physical security vulnerabilities of the kiosk system?			
• Are there policies in place to guard against physical security vulnerabilities and to protect kiosk hardware and components that hold e-PHI?			
• Are there procedures and policies in place to control access to kiosk hardware, systems and other components by staff, visitors etc. that could compromise the kiosk system as a whole?			
• Are there maintenance records for repairs and modification of physical components especially relating to security?			
12. Computer Component Use			
• Is there other computer hardware, like workstations and servers that manage the kiosk system?			
○ If yes, are there policies and documentation outlining specific workstations and servers and their functions and location?			
○ Is there documentation and procedures to identify specific functions of each workstation and server?			
13. Workstation and Server Security			
• Is there any policy or procedure to prevent unauthorized access to an unattended workstation or to limit the ability of un-authorized persons to access other users' information (analyze physical surroundings for physical attributes)?			

• How are workstations and servers physically restricted to limit or restrict access to only authorized people?			
14. Device and Media Controls			
• Is there any policy for monitoring and tracking the location and movement of kiosk hardware (especially containing e-PHI)?			
15. Access Control			
• Is there an access control policy?			
• Is there an encryption procedure in place to protect e-PHI?			
○ If yes, are there any well documented policies governing and outlining the encryption strategy?			

Access Control (Continued)			
• Are there any policies to make sure all users are assigned unique access credentials, like IDs and passwords, to log on to the kiosk system?			
• Are all users assigned usernames and passwords?			
• Is there documentation of each user's exact privileges in the kiosk system (useful to prevent privilege escalation)?			
• Are there clearly defined policies to track changes and modifications made within the kiosk system, including which users made the changes?			
• Are there any policies in place to make sure user access is reviewed on a periodic basis and how often that is done?			
• Is the system configured to auto-logoff after a predetermined time?			
○ Is there any documentation and defined policy for this?			
• Are there procedures for terminating access when it is no longer needed?			
16. Audit Control			
• Has any audit control been implemented?			
• Are there any audit control policies in place?			
• How often are the audit control tools and mechanisms reviewed to determine if upgrades are needed? ○ 0 times in a year? ○ Once a year? ○ Twice a year? ○ Three times a year? ○ More than three times a year?			

17. Integrity	Yes	NO	N/A
• Who has access to information or e-PHI stored in the kiosk systems?			
• Is there a well-defined policy or procedure to identify these individuals?			
18. Person or Entity Authentication			
• What kind of authentication procedure or mechanism is in place within the kiosk system?			
• Are there any policies to govern this and evaluate the authentication mechanisms in place to assess the strengths and weaknesses of the mechanism?			
○ If so does the policy also look at the cost benefit ratio of the various types of authentication mechanisms?			
• Is there a policy to test and upgrade the authentication mechanism tested on a periodic basis?			
19. Transmission Security			
• Is there any formal data transmission policy for the kiosk system?			
• Is there any risk assessment policy to determine the security level of the data transmission procedure in the kiosk system?			
• Is there a formal policy for breach notification?			
• Is there a template or letter or other defined means of breach notification?			
• Does the notification policy include procedure for notification of media outlets?			
• Does the policy also spell out notification procedures for Business Associates, if any?			

APPENDIX B: KIOSK PRIVACY AND SECURITY POLICIES

Kiosk Security Policies Last Updated_____

Purpose

This document defines the privacy and security policies for the "XYZ" Multi-user health kiosk system. We take all aspects of security of our system as well as the privacy and confidentiality of our users' data very seriously. To protect the overall multi-user health kiosk system and keeping user data and information private and confidential in compliance with HIPAA and HITECH rules, this policy must be fully implemented and adhered to.

Intent

The goal of this policy is to provide the kiosk project team and future administrators of the multi-user health kiosk system to meet privacy, security and confidentiality requirements of HIPAA, HITECH and other healthcare regulations. The content of this policy will reflect requirements listed in the Office for Civil Rights (OCR) audit protocol.

Scope

This policy applies to the entire multi-user health kiosk infrastructure. This includes but not limited to servers, network, databases, software, kiosk hardware, data at rest, and data in transit.

The policy also applies to workers and users who interact with the kiosk and any third-party companies that may create access or store any user data.

Audience

This policy covers all employees, management, contractors, vendors' business partners/associates and any party that may have access to any aspect of the multi-user health kiosk system.

Attributes of Information to be protected

A complete inventory of the multi-user health kiosk system should be conducted to determine what will need to be protected. This process should be completed any time a change is made to the kiosk system/infrastructure.

Definitions

Privacy

This is the ability for people to keep their personal information a secret from others. It is good to note that a breach of confidentiality will constitute a breach of privacy.

Confidentiality

This is a process to ensure that only authorized people can view the people's personal data.

Availability

This is making sure that information and other system resources are available, when needed, to all authorized users.

Access

The capacity/right to use, modify or manipulate an information resource to gain entry to a physical location.

Access Control

This is a procedure of approving or denying specific requests for obtaining and using information. This is to make sure only authorized people have access to IT/computer systems.

Principle of Least privilege

User Privilege to access and use any resources should be absolutely limited only to resources necessary to perform assigned duties and nothing else. This is important to prevent privilege escalation.

Principle of Separation of Duties

As much as possible to limit the potential for fraud, or fraudulent activities, one person should not be put in charge of completing any tasks from beginning to end. Multiple people must be assigned sections of the task to be completed.

Security Outline

Appropriate steps should be taken to protect all aspects of the multi-user health kiosk system; hardware, software and data/information with the kiosk system.

Security should therefore cover a wide range of security entities including:

- **Physical Security**
    - Access controls, DC controls, data disposal Methods, preventing access to internal kiosk components.
- **Logical Security**
    - Deals with user accounts & passwords
- **Servers & PCs**

- Software licenses, patch management (operating system and other security updates), laptop security.

- **Network Infrastructure**
  - Making sure there is a standby version for network components in case of outage, to reduce downtime (Core redundancy), Change Management, single point of failure

- **IT Security Policies, Procedures, Practices**
  - Security, acceptable use, Backup (BC)/Disaster Recovery (DR) planning, etc.

- **Internal Network Vulnerabilities**
  - Patch and firmware levels, password management, etc.

- **External Network Vulnerabilities**
  - Penetration testing, attack vulnerabilities, open ports.

- **File Backup & Recovery**
  - File backup and recovery procedures, offsite storage, and retention periods.

- **AV, Spyware, SPAM**
  - Protection, content filtering, Intrusion Detection System (IDS)/ Intrusion Prevention System (IPS).

- **Software Security**
  - Mission-critical apps, changes and updates, testing.

It is the responsibility of everyone who interacts with the multi-user health kiosk to protect the system including the data and all computer infrastructure of the k*i*osk.

Responsibility

All individuals including users' who interact with the kiosk system must comply with the contents of the policy and reporting of any actions that violates this policy in any way.

Administrators of the kiosk system are responsible for making sure any group of people that work with on the kiosk system understands the scope and implications of this policy.

Kiosk administrators should, on a continuous basis, monitor the entire kiosk system including data and update access requirements and other P&S requirements.

Management

Kiosk management shall be the owner of this security and should work with all others in charge of all the IT components of the kiosk to keep the system secured. All the various activities to secure the system will be in the detailed part of this policy.

Review

Kiosk management is responsible for keeping this policy current. The policy will be reviewed annually/quarterly, or any time there has been major changes in the kiosk system.

It is highly recommended to undertake a full security audit to make sure policies are well aligned with HIPAA, HITECH and other regulations.

Enforcement

Anyone found to be engaging in activities, unintentionally or intentionally that compromise the kiosk system in any way will be disciplined accordingly in conjunction with OCR rules.

Acknowledgement

Kiosk Management name: _____

Signature: _____

Witness Name: _____

Witness Signature: _____

Date: _____

Detailed Policies

Policy#	Explanation of Policy	Status		
		Completed? Yes/No	**N/A**	**Date Modified**
1.1	**Privacy Policy** **How your Information will be used:** User's private information including Protected Health Information (PHI), if it exists in the kiosk system will not be disclosed without authorization from the user. **Disclosure to Business Associates** When necessary, a user's personal information should only be made available to Business Associates (BAs) who have agreed in			

	writing to maintain the privacy of the information as required by law **Use or Disclosure Requiring Authorization** The multi-user health kiosk personnel should only disclose user's private information for only the purposes mentioned in this document. Written authorization or consent from the user will be obtained before disclosing any personal information for other reasons. **Revoking Authorization** Users can revoke written previous authorization at any time in writing. **Use or Disclosure Permitted by Law** Kiosk management/personnel may use or disclose users personal or protected information to the extent that that is permitted by law: • *Public Health:* For public health activities or as required by the public health authority.			

	• *Health Oversight:* To a health oversight agency for activities such as audits, investigations and inspections. Oversight agencies include, but are not limited to, government agencies that oversee the health care system, government benefit programs, other government regulatory programs and civil rights laws. • *Legal Proceedings:* In response to an order of a court or administrative tribunal, in response to a subpoena, discovery request or other lawful process. • *Law Enforcement:* For law enforcement purposes, including: – legal process or as otherwise required by law; – limited information requests for identification and location; – use or disclosure related to a victim of a crime; –*Criminal Activity:* As requested by law enforcement authorities, if the use or			

	disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public. **Use and Disclosure Examples** • *Payment:* Kiosk Management/personnel may use PHI for payment processing to verify that services provided were covered under the patient's vision care plan. • *Health Care Operations:* Kiosk Management/personnel may use and disclose PHI for audit purposes. • *Treatment:* To coordinate treatment by a health care provider. *Personal Representative:* Kiosk Management/personnel may disclose your PHI to a person who has legal authority to make health care decisions on your behalf. **Disclosure Requiring Opportunity to Object** Kiosk Management/personnel may disclose your PHI to a family member, friend, or			

	other person involved in your care or payment if the information is relevant to their involvement and you have agreed or had an opportunity to object. **User rights** A copy of this notice should be made available to all first-time kiosk users or upon user request.			
1.2.1	**Retention of Personal Information/PHI** HIPAA and HITECH requires all covered entities (CEs) and business associates (BAs) to retain most personal information including PHIs for at least 6 years. Some state regulations require and at least 7 years. For Multi-user health kiosk system the retention period will be not less than 8 years. The following actions will be taken in order to meet this requirement:			

	• There must be a designated person tasked to ensuring that records and information is retained for the required amount of time. • An inventory of all records to be retained, as well as the locations of such records, should be created. These records should then be backed up using appropriate back up procedures. • This backup should be kept separate from all other backups. • Where possible software tools such as IBM's software should be employed to categorize data that must be retained for HIPAA, HITECH and other regulations as well as the time period that these data sets must be kept.			

Policy#	Explanation of Policy	Status		
		Completed? Yes/No	N/A	Date Modified
1.2.2	**Disposal of PHI/ Personal information** All PHI and other information should be disposed of in accordance to HIPAA/ HITECH or state law. Where possible a third party should be hired to dispose of PHI and other confidential information after they have exceeded their retention period of 7 years. Paper based records should be shredded or place in special beans to be picked up by a third party company to be shredded. Electronic PHI should be disposed of by deleting and reformatting the magnetic or			

	electronic media like flash drives, CD-ROM drives, hard drives and other media on which such information is stored. Hard drives should be placed in a highly magnetized medium to make sure information could not be retrieved from such hard drives in a way or form. Hard drives from all computers should be replaced and the old ones destroyed before the computers are either reused or sold.			
2	**CONFIDENTIALITY**			
2.1	**Request of Information** Kiosk user permission must be sought before disclosing or sharing patient information with any third party; except in situations when the information is to be used to directly treat the user of billing. This			

	authorization must always be signed by the user.			

Policy#	Explanation of Policy	Status		
		Completed? Yes/No	**N/A**	**Date Modified**
3	**SECURITY**			
3.1	**Security Management Process** **Asset Inventory (Items to protect):** 1. Network (servers, switches, computer devices) This policy will depend on CMU network security policies since the backbone of the kiosk system is part of the Carnegie			

	Mellon University (CMU) network. 2. Kiosk Hardware (Hard-drives, USB ports, CD-ROM drives) 3. Kiosk Software and underlying operating systems 4. Kiosk database 5. Users and other human assets (Employees etc.) **Threat Sources:** 1. **Environmental** – external fires, HVAC failure/temperature inadequacy, water pipe burst, power failure/fluctuation, etc. **2. Human** – hackers, data entry, employees/ ex-employees, disgruntled workers, impersonation, malicious software, code or application, theft, SPAM, Phishing, vandalism, etc.			

	3. **Natural** – Fires, flooding, other natural disasters, etc. 4. **Technological** – Power outage, database problems, failure of computer components, etc. 5. **Other** – Quitting of employees, medical emergencies, misuse of privilege and resources, etc. 6. **Threat to users –** Identity theft, fraudsters, etc. **Vulnerabilities:** 1. Access to USB, CD-ROMs, and other internal components. 2. Keyboard function keys could be used to get to the underlying operating system. 3. Ability to gain access to the underlying operating system. 4. Theft of kiosk components. 5. Data at rest on the kiosk or in transmission could be compromised			

	6. Hacking and gaining access to kiosk database 7. Privilege escalation 8. Shoulder surfing 9. Network breach or intrusion 10. Data loss or corruption of data 11. Failure of computer components *Detail policies to minimize the impact of these vulnerabilities are highlighted in subsequent areas of the security section of this document.* **Risk Assessment Policy:** Risk assessment should be performed twice a year or when there is a major update of the kiosk system and other auxiliary computer components or system. **Audit Trail:** Audit trails can play a tremendous role in detecting security violations, performance problems, flaws in applications or software and trouble			

	shooting. Hence all user activities and other system and application processes must be preserved. All users on the kiosk system must be authenticated to allow for accountability of user actions. In addition, all administrative activities must be monitored to help in trouble shooting and resolving problems.			
3.2	**Assigned Security Responsibility** There should be a security officer whose job it will be to develop implement monitor and communicate HIPAA /HITECH policies and procedures to employees.			
3.3	**Workforce Security** To prevent privilege escalation and unauthorized access to all kiosk resources;			

	There should be documentation of the type of authorization and supervision for all entities working with the kiosk. This documentation shall include clear job description for all the people working with the kiosk and shall also state clearly the level of access each employee has to the kiosk systems and the data within the kiosk. All privileges to every Aspect of the kiosk including computers, servers and other kiosk network resources should be terminated and all user accounts disabled the moment a person stops working with the kiosk or is relieved of all duties associated with the kiosk.			
3.4	**Information Access Management** There must be clear documentation for granting access to sensitive information in the Multi-user			

	health kiosk systems. This must include clear procedure to authorize and document access, review and modify user's access to Multi-user health kiosk computer systems, software, databases and other network resources. All third parties that access and use any information in the Multi-user health kiosk systems must adhere to these procedures in accordance to HIPAA and HITECH security rules. **Identification:** To facilitate decision making on the level of access to be granted to individuals, unique identifiers must be assigned to every person who uses the Multi-user health kiosk. Identifiers or token must have the following attributes:			

	• Uniqueness, meaning each identifier (User ID, username etc.) must be uniquely associated to only one person. • No one person should have more than one account or identifier within the Multi-user health kiosk system. This makes it easier to implement audit trails. • There should be no reassignment of identifiers even if a person leaves, resigns or is terminated. Once an identifier is associated with a person it should never be reassigned to another person or individual. **Authentication:** This is the process of determining if a person, entity or thing is what it is said to be. So, authentication validates			

	the identity of a person or thing within the computer system. This process uses both a public and private identifier. The public identifier is usually the person's username or identification number assigned within the system and the private identifier is usually a Personal Identification Number (PIN), password or secrete code. The private identifier must never be shared or disclosed to anyone. Encryption authentication must be used, and should have the adhere to the following rules: • Credentials for authentication should never be incorporated into program codes or queries. The only exception is when no reasonable alternative exists. In			

	such situations, the authentication information must be encrypted. • Temporary or initial passwords must be communicated to intended users in a secure manner and user accounts must be configured to prompt for password to be changed on first or initial logon. • Refrain from storing passwords in reversible forms or in clear text. • Identify and reset all Vendor-supplied, default or blank passwords immediately following installation of applications/software, devices or operating systems. • All passwords must meet requirements for strong passwords:			

	Password Expiration → Every 180 Days Minimum Length → 12 Characters Password Complexity → Enabled Password History → Last 10 passwords Account Lockout → After 5 consecutive unsuccessful logon Attempts Lock-out Duration → 30 minutes Renewed Log In → After 30 minutes of inactivity or by a systems administrator Screensaver → Password protect when idle after 10 minutes **Authorization:** This is a way of granting authenticated users' permission to use information and resources. This			

	can be accomplished through the use of technology or process and determines what type of access (Read, Write, Create, modify, delete) that a user has to a resource. The system must be effective enough to verify if a particular user has the right to perform a given operation. All users must be prevented from having access to information or resource without proper authorization. Data access procedures must be clearly defined and should include: • The use of access request forms must be used to modify of delete existing privileges to			

	the Multi-user health kiosk systems • Users to the kiosk should be accorded the least privilege necessary to perform their assigned functions within the Multi-user health kiosk system. Privileges should be reviewed regularly and modified, suspended or deleted if a user's job function changes, gets transferred, resigns or is dismissed. • In the case of new account requests, must be completed and authorized by: I. The person requesting the access to the kiosk systems or resource. II. Supervisor or department head of the person requesting the			

	access must complete a portion of the form. III. The person who owns the data or the person who generated the data must also complete a portion of the form. • User accounts must be modified in a timely manner according to their new job description of privilege level matching their role when a worker is promoted or assumes new responsibilities. In situations where a worker is terminated with cause the accounts should be deactivated immediately. • Privileges must be reviewed to make sure user privileges match their current responsibilities. This allow accounts to be			

	modified, or deactivated when access is no longer needed. Management of the kiosk system will have to ensure that anyone who has access kiosk system is properly trained on how to interact with such data in compliance with HIPAA and HITEC rules. They should also be given copies of the kiosk privacy and security policies. **Segregation of Duties** Segregation of duties principle must be used to grant access privileges to individuals. For example, systems administrators should be given a separate/personal account that they will use to log on to the system for non-admin/ person business.			
	All third-party vendors who view or interact with the Multi-user health kiosk system and have access to any data in the kiosk			

	system should enter into a business associate agreement with the Multi-user health kiosk management.			
	There should be security officer who will constantly review HIPAA/HITECH and other federal and state regulations and train employees who administer components of the Multi-user health kiosk accordingly.			
	All computer systems and software forming part of the Multi-user health kiosk system should be updated frequently to protect against viruses, malware and other security threats. Anti-virus programs should be installed on all the kiosk computer system. For example, Sub-netting and firewalls can also be implemented to reduce the spread of viruses and other malware. Databases and Webpages should be protected against SQL injections and other attacks.			

	In other not to confuse people, security training materials should target security issues relevant to the Multi-user health kiosk system.			
	Security policies will be reviewed and updated quarterly in situations where there are no issues. If any issues occur or vulnerabilities are identified, then the issues should be investigated and resolved, and the security policy updated accordingly to protect against future occurrence.			
	All security breaches should be investigated and reported immediately. All malware infested computers should be taken off the network immediately to minimize the spread of the malware. If the security breach involves the loss or compromise of user's data in any way, the affected individuals must be noted, and steps should be taken to report the incident to the appropriate entity according to HIPAA and HITECH rules.			

3.5	**Contingency Plan** Steps must be taken to identify critical applications, data and other kiosk operations and components. This makes it easier to implement or put procedures and processes in place to restore and recovers services in case any of those components fail, gets damaged or stolen.			
	There should be a disaster recovery plan to restore data, hardware, and other components of the Multi-user health kiosk systems in case of a disaster. (disaster recovery plan details later) Disaster recovery plans must be tested quarterly to test their effectiveness and find a fix potential problem in the plan.			
3.6	**Evaluation** The security and privacy officer are responsible to review and evaluate kiosk security and privacy procedures to make sure they reflect standards set by HIPAA/HITECH			

	and other state agencies. The security and privacy officer will be responsible for creating and documenting procedures for evaluating security and privacy of the kiosk to make sure they comply with HIPAA/HITECH and other regulations.			
3.7	**Business Associate (BA) Contracts** All third-party vendors and contractors who interact with the kiosk must be required to sign a business associate agreement with the Multi-user health kiosk management.			
3.8	**Physical security** The physical location within which the kiosk is deployed must evaluated for probable security vulnerabilities. The kiosk must be deployed in a well-lit area, free of water and fire hazards and offer protection from vandals and other criminals. All internal, sensitive and vulnerable kiosk components must enclose in a secured and locked compartment attached to the kiosk			

	assembly to minimize threat posse by thieves, vandals and other criminals. Only administrators or kiosk management will have keys to the storage attached to the kiosk. When it is possible, there must be an attendant to supervise the use of the kiosk system. A log should also be kept of all maintenance activities and any physical modifications of the Multi-user health kiosk system.			
3.9	**Computer Component Use** Documentation of all kiosk computer component (workstation, servers, etc.), as well as their functions and location should be maintained. These computer components must be identified by their names and IP addresses This will help identify potential intrusion or breaches of the Multi-user health kiosk system.			

	All workstations, servers and other computer components must be configured to prompt users for usernames and passwords before they can access any resources. User should be logged of the screen saver activated if there is no activity for 15 minutes.			
3.10	**Workstation and Server Security** Access to workstations and servers must be physically restricted. Server should be locked in a dedicated room with the administrator and manger being the only people with keys. There should be administrator accounts to allow administrators to log on and perform access various resources on the multi-user health kiosk. There should be intrusion prevention mechanism installed on all computers. This provides the ability to lock the chassis/system box to prevent people from stealing computer components like hard drives etc.			

	In a situation where administrators want to access resources remotely this should be done through a secured VPN connection. VPN access must be managed through a special organization unit. This makes it easier for users to added or removed from the organization unit to give them access or disable access respectively. More detail on this should be based on CMU security policies on server and workstation security,			
3.11	**Device and Media Controls** This policy helps to meet HIPAA/HITECH requirement to limit PHI to those with a need to know. This should apply to receipt, movement, hardware removal or destruction. This should also cover installation or removal of hardware devices from the multi-user health kiosk and its computer systems.			

	There should be an inventory system for all kiosk hardware that is used to store users' personal information like e-PHI. There should also be a description of the person responsible for ensuring this policy. This documentation or inventory should contain: • A well-defined procedure for the destruction and disposal of hardware and other electronic media used to store PHI. It should also state clearly who is responsible to oversee this process. • A well-defined procedure for removal of PHI from reusable media like tapes, discs, CD-ROMs or Diskettes before they are reused. • A well-defined method for recording the movement and storage of hardware and electronic media into and out of the multi-user health kiosk system. There should be people responsible for documenting the receipt or removal of			

	hardware and electronic media to ensure that their location is known at all times. • Where necessary a copy of the data on the Multi-user health kiosk equipment should be made before the equipment is moved, and the procedure should be well documented. There should be a unique tracking number to help track the whereabouts of such devices at all times. • Where necessary a copy of the data on the multi-user health kiosk equipment should be made before the equipment is moved, and the procedure should be well documented. There should be a unique tracking number to help track the whereabouts of such devices at all times. • There should be a well-defined backup and restore procedure in place.			

	• They should be weekly full backups and daily deferential backups (to allow for faster restore during data loss or corruption) • Data that is more than five years should be archived and kept on backup tapes for 25 years. So, the same data is not backed up over and over again. This also helps to ensure that only the newest data is kept on line. • Full monthly backups should be taken, and backup tapes stored at an offsite location • In the situations where electronic media is reused, all previous data on such devices must be completely erased. • There must be a well-documented process for processing electronic media for reuse. There must be a designated person to oversee this process.			

3.12	**Access Control** This policy is to guard against unauthorized access to information and data generated within the kiosk systems. This includes data at rest and data in motion or in transit. This means the storage media on which the data is stored must be encrypted and the data itself must be encrypted before it is transmitted or moved across a computer network. Since HHS deferred to NIST for Cryptographic standards it is recommended to use the NIST standard (AES, Triple DES, and Skipjack) as a guide. • There must be an elaborate access control policy. • An acceptable encryption method comparable to the three encryption standards recommended by NIST should be employed in the Multi-user health kiosk system (Data Encryption			

	Standard (DES), Triple Data Encryption Algorithm (TDEA), and Advance Encryption Standard (AES)). • The encryption should protect the data at rest: Hard drives, removable drives (CD-ROM, USBs and portable hard drives) used to store data should be encrypted. • Encryption should also be employed to protect data in motion or transit: This means data that is being transmitted across a network should be encrypted. The data will then be protected in the event that it falls in the wrong hands or it is intercepted by a rouge person. • All user duties, responsibilities and access needs for all people who interact with the multi-user health kiosk must be identified and well documented. This procedure as well as the access			

	needs of all the various people must be well documented. • All kiosk users must have a unique identifier (Username and Password) to allow user activities within the system to be logged and tracked. There must be documentation of how this is done. • There must be an administrator of the kiosk who has the right to add, modify and delete user access. This must be reviewed on a periodic basis and updated when users job responsibilities change or when users are no longer working on the multi-user health kiosk. • As part of this procedure, the computers must be configured auto log off when the system is not in use for a period of time. • There should be thorough documentation to serve as a directive for this policy.			

3.13	**Audit Control** There should be a well-documented procedure for performing security audits of the kiosk system. This is to serve as a guide for performing security audits of the kiosk system. Audits are necessary to ensure integrity, confidentiality, and availability of information and resources. This is to protect the system against: • Access to confidential data • Unauthorized access to the multi-user health kiosk computers • Sharing or compromising people's passwords • Out of date anti-virus definition files • Denial of service (DOS) attacks • Unsecured network access from the outside world including open ports and badly configured			

	network devices (routers, modems, switches etc.) • The audits should be performed semiannually.			
3.14	**Integrity** This part of the security policy is to protect the accuracy and constituency of data in the multi-user health kiosk system. • Data must be stored, accessed and transmitted in a secured manner in order to maintain data accuracy and consistency. • Only kiosk administrators must have the privilege to delete or modify data. • Steps must also be taken to minimize the possibility of man- in-the-middle attack by transmitting data in a secured manner. This procedure must me well documented.			

APPENDIX C: PRIVACY AND SECURITY POLICY STATEMENT FOR STUDY 2 (SAMPLE)

To protect the information, you provide at the health kiosk and to ensure that the kiosk is secure, the following measures are in place:

1. Rules are being followed from two laws:
    a. the Health Insurance Portability and Accountability Act (HIPAA)
    b. the Health Information Technology for Economic and Clinical Health Act
2. The Office for Civil Rights enforces the HIPAA and HITECH laws. Its standards and audit protocols guide the policies we have in place to protect your security, privacy, and confidentiality related to the health kiosk.
3. All parts of the health kiosk are locked down to prevent access by people without permission.
4. We make every effort to make sure the health kiosk is placed where it would be difficult for others to read your information on the screen.
5. Every person who uses the health kiosk must access his or her account using a unique key fob and password. No kiosk user may access anyone else's account.
6. No user data is stored at the health kiosk. Instead it is sent directly to a secure computer storage system at the University of Pittsburgh.

7. All your responses and measurements obtained at the health kiosk are labeled with a unique code number. That way, your private information cannot be linked to your name by anyone else using the kiosk.
8. Information sent in reports to your primary care provider is done only with your permission.
9. Based on the consent you provided to take part in this Health Kiosk Study, members of the Health Kiosk Project team may see your kiosk data only for the purposes of the study.
10. Members our team always keep your information private and secure.
11. Up-to-date antivirus and anti-malware software are on the kiosk computer system at all times.
12. When a member of our team stops working on the Health Kiosk Project, his or her kiosk account is disabled right away.
13. The health kiosk system is regularly checked to ensure that all security, privacy and confidentiality policies for the kiosk are being met.
14. Data gathered through our health kiosk is backed up daily to prevent data loss in case of system failure or natural disaster such as a flood, fire, or power outage.

APPENDIX D: SECURITY AND PRIVACY SURVEY QUESTIONS

Name: **Participant #**

What is your educational level?
____Less than High School
____High School /GED
____Some College
____College

How would you rate your computer skill level?
_____Never used a computer
_____Beginner
_____Competent

Security and Privacy Questions

Please circle the number to show your level of agreement with each statement below:

Security:

Security refers to protecting the equipment, software, and information gathered or provided by persons using the health kiosk.

	Strongly Disagree	Disagree	Neither Agree/ Disagree	Agree	Strongly Agree
1. The information I provide at the kiosk is secure due to the key fob and password I use to get to my account.	1	2	3	4	5
2. The kiosk safely transfers my information to the University of Pittsburgh.	1	2	3	4	5
3. The kiosk is placed in a safe location.	1	2	3	4	5

4. I trust the kiosk and the personnel who work with it.	1	2	3	4	5
5. I am satisfied with the overall security of the kiosk.	1	2	3	4	5
6. The kiosk does a good job of protecting my information from people who should not have it.	1	2	3	4	5
7. All my personal information at the kiosk is kept safe so that people who should not see it cannot see it.	1	2	3	4	5

Privacy:

Privacy protection is about keeping personal information secret from others. Confidentiality refers to ensuring that only authorized people can view a person's personal data. Breach of confidentiality occurs when a person's information is viewed or shared with others without that person's consent. A breach of confidentiality *is* a breach of privacy.

	Strongly Disagree	Disagree	Neither Agree/ Disagree	Agree	Strongly Agree
8. The kiosk respects my privacy rights when obtaining personal information.	1	2	3	4	5

9. The kiosk design shows concern for the privacy of its users.	1	2	3	4	5
10. The kiosk only collects personal data from me that are necessary.	1	2	3	4	5
11. Using the kiosk does not put my privacy at risk.	1	2	3	4	5
12. I feel that it is safe to enter my personal information at the kiosk.	1	2	3	4	5
13. The kiosk appears to abide by personal data protection laws.	1	2	3	4	5
14. I am confident that the personal information I provide at the health kiosk is not shared with others without my consent.	1	2	3	4	5
15. The kiosk prevents people who should not have my	1	2	3	4	5

personal information from accessing it.					
16. From the modules listed below, rank the ones that you believe are extremely private (5) to not so private (1)					
A. *Bladder Health*	1	2	3	4	5
B. *Lifestyle*	1	2	3	4	5
C. Sleep	1	2	3	4	5
D. Patient-Provider Communication:	1	2	3	4	5
E. Mood	1	2	3	4	5
F. Mobility and Balance:	1	2	3	4	5
G. Lifestyle	1	2	3	4	5
H. Physical activity and	1	2	3	4	5
I. nutrition	1	2	3	4	5

17. Intention to use:

Refers to a state of mind that drives an individual to use or not to use the kiosk

Do you intend to use the kiosk?

Yes☐ **No ☐**

If you answered no, can you please provide a brief explanation for your answer?

Questionnaire References:

(Flavián & Guinalíu, 2006; C.-F. Li, 2013; Lwin, Wirtz, & Williams, 2007; Okazaki, Castañeda, Sanz, & Henseler, 2012)

APPENDIX E: SCORING OF CHECKLIST FOR MULTI-USER HEALTH KIOSK

HIPAA/HITECH Compliance Checklist for Multi-User Health Kiosk			
PRIVACY	Yes	NO	N/A
Personal Information			
• Is there a privacy policy?	X		
• Does the kiosk have a privacy screen?	X		
• Will user information be shared with third-party companies?			X
• If yes, is there a Business Associate (BA) agreement with this company?			
Retention of Personal Information			
• Is user information and e-PHI stored?	X		
• Is there a policy outlining the retention period of e-PHI?	X		
• Can users request copies of their Information?			
• If yes, is there a well-defined procedure for requesting copies of PHI and other information?			X
CONFIDENTIALITY			
Request of Information			
• Is there a policy for disclosure of e-PHI or identifiable information?	X		
SECURITY			
Security Management Process			

• Is there a well-written procedure or protocol for performing a thorough risk assessment?	X		
How many times in a year is a risk assessment performed? o 0 times in a year? o Once a year? o Twice a year? o Three times a year? o More than three times a year?			
• Is there a formal or informal policy or procedure to review information system activities like audit logs, access reports incident tracking etc.?	X		
• Are current security measures sufficient to reduce risk and vulnerabilities to a reasonable level?	X		
Assigned Security Responsibility			
• Do you have a security officer in charge of developing, implementing, monitoring and communicating HIPAA/HITECH security policies and procedures?	X		
Workforce Security			
• Do you have documentation for authorization and supervision of all entities working with or helping to manage and maintain the kiosk?	X		
• Do you have clear job descriptions for all entities working with the kiosk?	X		
• Is there documentation listing the level of access to the system, including e-PHI for each employee?	X		
• Is there a clear procedure to terminate access to resources once a person is removed from the project or terminated?	X		
Information Access Management			
• Is there a clear written procedure to grant access to e-PHI?		X	
• Do policies and standards exist to authorize and document access, review and modify a user's right to computer systems, software, databases and other network resources?	X		
• Are users going to pay to use the kiosk system? o If so, will a clearinghouse or third party be used to process payment? ▪ If so, are there policies and procedures for access to information, by clearinghouse workers, consistent with HIPAA and HITECH security rules?			X

• Are formal or informal policies and procedures in place for security measures relating to access control?	X		
• Is there any HIPAA and HITECH security awareness and training program in place?		X	
• Are there procedures and measures in place for protection from malicious software and exploitation of vulnerabilities?	X		
• Have employees been trained as to the importance of protecting against malicious software and how to guard against it?			X
• Are there policies and procedures for log–on monitoring and password management?	X		
• Do security training materials target current IT security topics relevant to kiosk security?			X
How often are security procedures, policies and protocols updated? o 0 times in a year? o Once a year? o Twice a year? o Three times a year? o More than three times a year?			
• Are there any policies and procedures in place to identify, respond to, report and mitigate security incidents?	X		
Contingency Plan			
• Is there a contingency plan in place to identify critical applications, data and other operations of the kiosk system?	X		
• Is there a disaster recovery and backup plan in place to restore lost data?	X		
• Is any redundancy built into the kiosk deployment?	X		
• Is there any well-defined policy for operating in emergency mode that allows continuation of critical business processes?	X		
• Are there any policies for testing emergency contingency plans or backup procedures?		X	
Evaluation			
• Are there policies in place for evaluating the security procedures as they apply to HIPAA/HITECH security rules?	X		
Business Associate (BA) Contracts			

• Is there a policy for contracts with Business Associates and other third-party vendors?			X
Physical Security			
• Are there policies in place to analyze physical security vulnerabilities of the kiosk system?	X		
• Are there policies in place to guard against physical security vulnerabilities and to protect kiosk hardware and components that hold e-PHI?	X		
• Are there procedures and policies in place to control access to kiosk hardware, systems and other components by staff, visitors etc. that could compromise the kiosk system as a whole?	X		
• Are there maintenance records for repairs and modification of physical components especially relating to security?			X
Computer Component Use			
• Is there other computer hardware, like workstations and servers that manage the kiosk system?	X		
• If yes, are there policies and documentation outlining specific workstations and servers and their functions and location?			X
• Is there documentation and procedures to identify specific functions of each workstation and server?			X
Workstation and Server Security			
• Is there any policy or procedure to prevent unauthorized access to an unattended workstation or to limit the ability of un-authorized persons to access other users' information (analyze physical surroundings for physical attributes)?	X		
• Are workstations and servers physically restricted to limit or restrict access to only authorized people?	X		
Device and Media Controls			
• Is there any policy for monitoring and tracking the location and movement of kiosk hardware (especially containing e-PHI)?			X

Access Control			
Integrity	Yes	NO	N/A
• Is there an access control policy?	X		
• Is there an encryption procedure in place to protect e-PHI?	X		
• If yes, are there any well documented policies governing and outlining the encryption strategy?	X		
Access Control (Continued)			
• Are there any policies to make sure all users are assigned unique access credentials, like IDs and passwords, to log on to the kiosk system?	X		
• Are all users assigned usernames and passwords?	X		
• Is there documentation of each user's exact privileges in the kiosk system (useful to prevent privilege escalation)?	X		
• Are there clearly defined policies to track changes and modifications made within the kiosk system, including which users made the changes?			X
• Are there any policies in place to make sure user access is reviewed on a periodic basis and how often that is done?	X		
• Is the system configured to auto-logoff after a predetermined time?	X		
• Is there any documentation and defined policy for this?	X		
• Are there procedures for terminating access when it is no longer needed?		X	
Audit Control			
• Has any audit control been implemented?	X		
• Are there any audit control policies in place?	x		
How often are the audit control tools and mechanisms reviewed to determine if upgrades are needed? o 0 times in a year? o Once a year? o Twice a year? o Three times a year?			

○ More than three times a year?			

APPENDIX F: SCRIPT OF EXPLANATION OF PRIVACY AND SECURITY POLICY STATEMENT FOR STUDY 2 (SAMPLE)

To protect the information, you provide at the health kiosk and to ensure that the kiosk is secure, the following measures are in place:

1. Rules are being followed from two laws:
    a. the Health Insurance Portability and Accountability Act (HIPAA)
    b. the Health Information Technology for Economic and Clinical Health Act (HITECH)

Explanation to statement

HIPAA was enacted to protect people data and privacy and was later extended to HITECH to give it more bite. Violation could result in severe penalties (jail time and severe fines). The kiosk project is bound by HIPAA and HITECH to take steps to protect your personal data, privacy and confidentiality.

2. The Office for Civil Rights enforces the HIPAA and HITECH laws. Its standards and audit protocols guide the policies we have in place to protect your security, privacy, and confidentiality related to the health kiosk.

Explanation to statement

3. All parts of the health kiosk are locked down to prevent access by people without permission.

Explanation to statement

This prevents unauthorized people from stealing components like data storage systems that might have user information. It also prevents unauthorized people from installing secrete devices that can be used to steal personal/sensitive information from the kiosk.

4. We make every effort to make sure the health kiosk is placed where it would be difficult for others to read your information on the screen.

Explanation to statement

This is to prevent people from reading other people's information on the screen of the kiosk during kiosk usage.

5. Every person who uses the health kiosk must access his or her account using a unique key fob and password. No kiosk user may access anyone else's account.

Explanation to statement

Each user's key fob and password are linked to only their personal data, so they cannot access another person's personal information. Think of it as your bank card. Only you can use your bank card and your pin to access your account on an ATM.

6. No user data is stored at the health kiosk. Instead it is sent directly to a secure computer storage system at the University of Pittsburgh.

Explanation to statement

This limits access to your personal data in the event of a breach on the kiosk. It also allows a copy of your data to be created (backed up) to prevent data loss in the event of any failure of a computer component.

7. All your responses and measurements obtained at the health kiosk are labeled with a unique code number. That way, your private information cannot be linked to your name by anyone else using the kiosk.

Explanation to statement

All information that is obtained on the kiosk is de-identified (meaning no unauthorized people can link that information to you). This ensures that your personal information is kept private and confidential.

8. Information sent in reports to your primary care provider is done only with your permission.

Explanation to statement

Your approval/ consent will always be sought before any of your information is shared or made available to anyone including your primary care physician.

9. Based on the consent you provided to take part in this Health Kiosk Study, members of the Health Kiosk Project team may see your kiosk data only for the purposes of the study.

Explanation to statement

People working on the project are only allowed to use your personal information only for the study and nothing else.

10. Members our team always keep your information private and secure.

Explanation to statement

The project team are not allowed under any circumstance to share or make your personal information available to anyone

11. Up-to-date antivirus and anti-malware software are always on the kiosk computer system.

Explanation to statement

Anti-virus and anti-malware software must be kept up-to-date or current. This will prevent viruses and hackers from gaining access to the kiosk computer systems.

12. When a member of our team stops working on the Health Kiosk Project, his or her kiosk account is disabled right away.

Explanation to statement

This ensures that people who are no longer working on the project do not have access to the kiosk computer systems, your personal information and data.

13. The health kiosk system is regularly checked to ensure that all security, privacy and confidentiality policies for the kiosk are being met.

Explanation to statement

Periodic audits will be performed to make sure all the security and privacy configurations of the kiosk are up-to-date. This will also make sure all employees, and everyone involved in the kiosk project are keeping up with the security and privacy requirements of the kiosk.

14. Data gathered through our health kiosk is backed up daily to prevent data loss in case of system failure or natural disaster such as a flood, fire, or power outage.

Explanation to statement

A good backup and recovery strategy must be put in place to protect the kiosk data and your personal information. This allows us to have a copy of your personal data just in case there is a failure of the computer systems used to store your data.

APPENDIX G: SNIPPET OF RANDOMIZATION WORKSHEET

A	B	C	D	E	F
	Envelope Number	Study Group			
	1	A	1014	1014	
	2	B	1015		
	3	c	1018		
	4	A	1017		
	5	B	1019		
	6	C	2012	2012	
	7	B	4003	4003	
	8	C	3005		
	9	A	3003		
	10	C	1020	1020	
	11	B	3002	3002	
	12	A	3006	3006	
	13	B	3009	3009	
	14	A	4005		
	15	C	6002		
	16	A	2015	2015	
	17	C	2009		
	18	B	4004	4004	
	19	A	6001		
	20	B	6003	6003	
	21	C	2016		
	22	C	1024		
	23	B			
	24	A	1022		
	25	C	5002	5002	
	26	B	5003		
	27	A	1032		

APPENDIX H: TABLE SHOWING PARTICIPANTS "INTENT TO USE" RESPONSES

	A	B	C	D	E
1	Paticipant ID	Group ID	PR-Intent-to-use (yes=2 No=1)	PS-Intent-to-use (yes=2 No=1)	
2	1014	1	2	2	
3	3006	1	2	2	
4	2015	1	2	2	
5	6011	1	2	2	
6	4010	1	2	2	
7	6005	1	2	2	
8	1036	1	2	2	
9	4014	1	2	2	
10	1039	1	2	2	
11	8006	1	2	2	
12	5010	1	2	2	
13	4016	1	2	2	
14	4008	1	2	2	
15	7009	1	2	2	
16	4003	2	2	2	
17	3002	2	2	2	
18	6003	2	2	2	
19	4004	2	2	2	
20	1029	2	2	2	
21	6004	2	2	2	
22	6013	2	2	2	
23	7008	2	2	2	
24	7010	2	2	1	
25	8007	2	2	2	
26	8011	2	2	2	
27	8013	2	2	2	
28	1020	3	2	2	
29	2012	3	2	2	
30	2016	3	2	2	
31	5002	3	2	2	
32	5009	3	2	2	
33	6007	3	2	2	
34	4013	3	2	2	
35	1040	3	2	2	
36	8003	3	2	2	
37	7011	3	2	2	
38					
39					
40					

GLOSSARY OF TERMS

Terminology	Definition
Availability	Information should be available to authorized users all the time and in a timely manner
Bluesnarfing	Is the unauthorized access of information from a wireless device through a Bluetooth connection, often between phones, desktops, laptops, and PDAs (personal digital assistant)
Click Jacking	Is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages
Communications Security	ways to protect organizations operations or activities
Communications Security	Protection of medium of communication. Examples are encryption, secure transferee protocols like HTTPS
Confidentiality	To ensure that only authorized users can view the information
Default accounts	Administrator accounts created to allow initial setup and configuration of computer software and devices. These accounts are supposed to be disabled after initial setup
External and Internal users	External users are like clients who use the system and Internal users are like employees
External Network Vulnerabilities	Network vulnerabilities from external sources like Hackers, Spammers, viruses, cross site scripting and information leakage.
Integrity	Information is legitimate and that no authorized or unauthorized person, malicious software, has falsely or illegally altered the information
Internal Network Vulnerabilities	Network vulnerabilities that come from internal sources obsolete network devices and software applications, inefficient password management, privilege escalation

IT Security Policies, Procedures, Practices- developing and implementing	Privacy, acceptable use, Backup (BC)/Disaster Recovery (DR) planning and policies
Logical security	Measures to secure software, computer applications, operating systems, databases, passwords and other user information.
Malware	Short term for malicious software, it can be used to disrupt computer operations, steal sensitive information. EG Viruses, Trojan horses, rootkits
Non-repudiation	This is to ensure that the origin of the message is legitimate.
Personnel security	Measures taken to protect workers; like having security guards and ID cards
Physical security	Physical mean of protecting computer systems. Examples are locks, security guards, concealing network and other computer cables.
Privacy	Ability for people to keep their personal information secret from others
Risk	ISO 13335 – Information Technology Security Techniques defines "risk" as: The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization
Rootkit	Is a stealthy type of software, typically malicious, designed to hide the existence of certain processes or programs from normal methods of detection and enable continued privileged access to a computer system?
RSE	Short form for Reverse Social Engineering. It is techniques used to trick a people to provides person/ sensitive information
Servers & PCs	Software license management, patch management, device security (portable security)
Software Security	This include measure to protect software like installing anti- malware software like antivirus software
Threat	The Oxford Dictionary defines threat (noun) as 1 a stated intention to inflict injury, damage, or other hostile action on someone. 2 a person or thing likely to cause damage or danger. 3 the possibility of trouble or danger.

Vulnerability **Vulnerability (continued)**	NIST SP 800-30 – Risk Management Guide for Information Technology Systems – defines a vulnerability similarly: A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.
Weak password	Passwords that do not meet password complexity requirements (at least 8 character long, include special characters, uppercase and lowercase, not a nickname)

BIBLIOGRAPHY

Abbott, E. B. (2010). Legal, Regulatory, and Social Challenges of Telemedicine and Mobile Health (mHealth).

Abdelmaboud, A., Jawawi, D. N., Ghani, I., Elsafi, A., & Kitchenham, B. (2015). Quality of service approaches in cloud computing: A systematic mapping study. *Journal of Systems and Software, 101*, 159-179.

Abdulhamid, S. M., Ahmad, S., Waziri, V. O., & Jibril, F. N. (2014). Privacy and National Security Issues in Social Networks: The Challenges. *arXiv preprint arXiv:1402.3301*.

Act, H. (2010). Health Information Technology for Economic and Clinical Health.

Addo, I. D., Ahamed, S. I., & Chu, W. C. (2014). *A Reference Architecture for High-Availability Automatic Failover between PaaS Cloud Providers.* Paper presented at the Trustworthy Systems and their Applications (TSA), 2014 International Conference on.

Adhikari, R., Richards, D., & Scott, K. (2014). *Security and Privacy Issues Related to the Use of Mobile Health Apps*.

Agarwal, N., & Sebastian, M. (2014). *Wireless infrastructure setup strategies for healthcare.* Paper presented at the Proceedings of the 7th International Conference on PErvasive Technologies Related to Assistive Environments.

Ahlan, A. R., & Ahmad, B. I. e. (2015). An overview of patient acceptance of Health Information Technology in developing countries: a review and conceptual model. *SciKA-Association for Promotion and Dissemination of Scientific Knowledge*.

Akshay, M., Kakkar, A., Jayasree, K., Prudhvi, P., & Metgal, P. S. (2015). Security Analysis in Cloud Environment. In *Artificial Intelligence and Evolutionary Algorithms in Engineering Systems* (pp. 221-228): Springer.

Algarni, A., Xu, Y., Chan, T., & Tian, Y.-C. (2014). *Social engineering in social networking sites: how good becomes evil.* Paper presented at the Proceedings of The 18th Pacific Asia Conference on Information Systems (PACIS 2014).

Ali, O., Shrestha, A., Soar, J., & Wamba, S. F. (2018). Cloud computing-enabled healthcare opportunities, issues, and applications: A systematic review. *International Journal of Information Management, 43*, 146-158.

Angst, C. M., Block, E. S., D'Arcy, J., & Kelley, K. (2017). When do IT security investments matter? Accounting for the influence of institutional factors in the context of healthcare data breaches. *MIS Quarterly, 41*(3), 893-916.

Annas, G. J. (2003). HIPAA regulations—a new era of medical-record privacy? *New England Journal of Medicine, 348*(15), 1486-1490.

Anthony, C. A., Polgreen, L. A., Chounramany, J., Foster, E. D., Goerdt, C. J., Miller, M. L., . . . Polgreen, P. M. (2015). Outpatient Blood Pressure Monitoring using Bi-directional Text Messaging. *Journal of the American Society of Hypertension*.

Appelt, D., Nguyen, D. C., & Briand, L. (2015). *Behind an Application Firewall, Are We Safe from SQL Injection Attacks?* Paper presented at the IEEE International Conference on Software Testing, Verification and Validation (ICST).

Awad, I. A. (2015). Security and Privacy.

Balebako, R., Marsh, A., Lin, J., Hong, J., & Cranor, L. F. (2014). *The Privacy and Security Behaviors of Smartphone App Developers.* Paper presented at the Workshop Usable Security.

Ballmann, B. (2015). *Understanding Network Hacks: Attack and Defense with Python*: Springer.

Basu, P., & Kanchanasut, K. (2015). Multicast Push Caching System. *Asian Institute of Technology*.

Bele, S. (2018). A COMPREHENSIVE STUDY ON CLOUD COMPUTING.

Bendix, J. (2013). What the HIPAA Omnibus rule means for your practice. *Contemporary OB/GYN website. http://images2.advanstar.com/PixelMags/obgyn/pdf/2013-06.pdf. modernmedicine. com/contemporary-obgyn/news/what-hipaa-omnibus-rule-means-your-practice. Published June, 1*.

Beretas, C. (2018). Security and Privacy in Data Networks. *Sensors, 1*(1), 1-20.

Bhuyan, S. S., Kim, H., Isehunwa, O. O., Kumar, N., Bhatt, J., Wyant, D. K., . . . Dasgupta, D. (2017). Privacy and security issues in mobile health: Current research and future directions. *Health policy and technology, 6*(2), 188-191.

Bilge, L., Strufe, T., Balzarotti, D., & Kirda, E. (2009). *All your contacts are belong to us: automated identity theft attacks on social networks.* Paper presented at the Proceedings of the 18th international conference on World wide web.

Bindahman, S., & Zakaria, N. (2011). Privacy in Health Information Systems: A Review. *Informatics Engineering and Information Science*, 285-295.

Bishop, M. (2003). What is computer security? *Security & Privacy, IEEE, 1*(1), 67-69.

Blumenthal, D. (2009). Stimulating the adoption of health information technology. *New England Journal of Medicine, 360*(15), 1477-1479.

Bouguettaya, A., & Eltoweissy, M. (2003). Privacy on the Web: Facts, challenges, and solutions. *Security & Privacy, IEEE, 1*(6), 40-49.

Bouzidi, M. R., Soltani, A., Bouhank, A., & Daoudi, M. (2018). *New Search Based Methods to Solve Workflow Scheduling Problem in Cloud Computing.* Paper presented at the 2018 5th International Conference on Control, Decision and Information Technologies (CoDIT).

Bowen, D. J., Kreuter, M., Spring, B., Cofta-Woerpel, L., Linnan, L., Weiner, D., . . . Fabrizio, C. (2009). How we design feasibility studies. *American journal of preventive medicine, 36*(5), 452-457.

Britton, K. E., & Britton-Colonnese, J. D. (2017). Privacy and security issues surrounding the protection of data generated by continuous glucose monitors. *Journal of diabetes science and technology, 11*(2), 216-219.

Brown, G., Howe, T., Ihbe, M., Prakash, A., & Borders, K. (2008). *Social networks and context-aware spam.* Paper presented at the Proceedings of the 2008 ACM conference on Computer supported cooperative work.

Buckovich, S. A., Rippen, H. E., & Rozen, M. J. (1999). Driving Toward Guiding Principles A Goal for Privacy, Confidentiality, and Security of Health Information. *Journal of the American Medical Informatics Association, 6*(2), 122-133.

Bugiel, S., Davi, L., Dmitrienko, A., Fischer, T., Sadeghi, A.-R., & Shastry, B. (2012). *Towards taming privilege-escalation attacks on Android.* Paper presented at the Proceedings of the 19th Annual Symposium on Network and Distributed System Security.

Bui, T., Wang, T., & Clemons, E. (2017). *Introduction to Information Security And Privacy Minitrack.* Paper presented at the Proceedings of the 50th Hawaii International Conference on System Sciences.

Burkhart, C. (2012). Medical Mobile Apps and Dermatology. *Cutis (Cutaneous Medicine for the Practitioner)*.

Cain, J. (2008). Online social networking issues within academia and pharmacy education. *American Journal of Pharmaceutical Education, 72*(1).

Canada, G. o. (2018). Types of survey questions. Retrieved from https://canadabusiness.ca/business-planning/market-research-and-statistics/conducting-market-research/types-of-survey-questions/

Cardenas, A., Amin, S., Sinopoli, B., Giani, A., Perrig, A., & Sastry, S. (2009). *Challenges for securing cyber physical systems.* Paper presented at the Workshop on future directions in cyber-physical systems security.

Care-Innovations. (2013). Older Populations Have Adopted Technology for Health. https://resources.careinnovations.com/hs-fs/hub/453282/file-2516634380-pdf

Carman, A. (2018). Google is shutting down Google+ for consumers following security lapse. Retrieved from https://www.theverge.com/2018/10/8/17951890/google-plus-shut-down-security-api-change-gmail-android#comments

Carr, N. (2013). Rough Type. Retrieved from http://www.roughtype.com/

Castro, D., Atkinson, R., & Ezell, S. (2010). Embracing the self-service economy. *Available at SSRN 1590982*.

Caves, E. J., Altarac, H., & Ilgun, K. (2008). Filtering subscriber traffic to prevent denial-of-service attacks. In: Google Patents.

Celebi, L. S., Joseph, G., Bilange, E. P., Marx, P. S., & Conroy, C. S. (2015). METHOD AND SYSTEM FOR ASSOCIATING INTERNET PROTOCOL (IP) ADDRESS, MEDIA ACCESS CONTROL (MAC) ADDRESS AND LOCATION FOR A USER DEVICE. In: US Patent 20,150,032,905.

Chadwick, S. (2014). Introduction. In *Impacts of Cyberbullying, Building Social and Emotional Resilience in Schools* (pp. 1-10): Springer.

Chambers, N., Fry, B., & McMasters, J. (2018). *Detecting Denial-of-Service Attacks from Social Media Text: Applying NLP to Computer Security.* Paper presented at the Proceedings of the 2018 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, Volume 1 (Long Papers).

Chaput, B. (2013). Truth-about-HIPAA-HITECH-and-Data-Backup. Retrieved from datamountain.com website: http://abouthipaa.com/wp-content/uploads/Truth-about-HIPAA-HITECH-and-Data-Backup_Article_2010-04-12.pdf

Charness, N., & Boot, W. R. (2009). Aging and information technology use potential and barriers. *Current Directions in Psychological Science, 18*(5), 253-258.

Choi, Y. B., Capitan, K. E., Krause, J. S., & Streeper, M. M. (2006). Challenges associated with privacy in health care industry: implementation of HIPAA and the security rules. *Journal of Medical Systems, 30*(1), 57-64.

Chou, D. C. (2015). Cloud computing: A value creation model. *Computer Standards & Interfaces, 38*, 72-77.

Christiansen, J. R. (2013). HIPAA/HITECH Compliance: Using the OCR Audit Protocols. Retrieved from http://christiansenlaw.net/2012/09/hipaahitech-compliance-using-the-ocr-audit-protocols/

Christodorescu, M., Sailer, R., Schales, D. L., Sgandurra, D., & Zamboni, D. (2009). *Cloud security is not (just) virtualization security: a short paper*. Paper presented at the Proceedings of the 2009 ACM workshop on Cloud computing security.

Ciampa, M. (2008). *Security+ Guide to Network Security Fundamentals, 1 yr*: Cengage Learning.

Ciampaglia, G. L., Shiralkar, P., Rocha, L. M., Bollen, J., Menczer, F., & Flammini, A. (2015). Computational fact checking from knowledge networks. *arXiv preprint arXiv:1501.03471*.

Coco, G. L., Maiorana, A., Mirisola, A., Salerno, L., Boca, S., & Profita, G. (2018). Empirically-derived subgroups of Facebook users and their association with personality characteristics: a Latent Class Analysis. *Computers in Human Behavior, 86*, 190-198.

Coe, R. (2002). It's the effect size, stupid: What effect size is and why it is important.

Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. In: Elsevier.

Corritore, C. L., Wiedenbeck, S., Kracher, B., & Marble, R. P. (2012). Online trust and health information websites. *International Journal of Technology and Human Interaction, 8*, 92+.

Craig, P. (2008). Hacking Internet Kiosk's. http://archive.hack.lu/2008/Craig_Hacking%20Kiosks.pdf

Cuckler, G. A., Sisko, A. M., Poisal, J. A., Keehan, S. P., Smith, S. D., Madison, A. J., . . . Hardesty, J. C. (2018). National health expenditure projections, 2017–26: despite uncertainty, fundamentals primarily drive spending growth. *Health Affairs, 37*(3), 482-492.

Curran, J. M., & Meuter, M. L. (2005). Self-service technology adoption: comparing three technologies. *Journal of Services Marketing, 19*(2), 103-113.

D'ESTE, G., & Taylor, M. A. (2003). *Network vulnerability: an approach to reliability analysis at the level of national strategic transport networks*. Paper presented at the Network

Reliability of Transport. Proceedings of the 1st International Symposium on Transportation Network Reliability (INSTR).

Dadkhah, M., Beck, M., & Jazi, M. D. (2014). Cross Site Scripting Vulnerability in Web Application: Review and Preventive Approach. *Journal of Applied Sciences Research, 10*(8).

Danish, M., & Sharma, P. (2018). Review Study of Cloud Computing–Benefits, Risk, Challenges and Security.

Das, I. (2014). *Studies of Privacy Issues in Online Social Networks.* Jadavpur University Kolkata,

Das, S., & Mukhopadhyay, A. (2011). Security and Privacy Challenges in Telemedicine.

Derek Fretheim. (2008). ADA Law and Self-Service Kiosks. Retrieved from http://k.b5z.net/i/u/2182899/f/ADA_Compliance.pdf

Dhanalakshmi, R., & Thomas, R. (2015). Prediction Model for Input Validation Vulnerabilities in Cloud Based SaaS Web Applications.

Dhote, H., & Bhavsar, M. D. (2018). Practice on Detecting Malware in Virtualized Environment of Cloud.

Ding, X., Verma, R., & Iqbal, Z. (2007). Self-service technology and online financial service choice. *International Journal of Service Industry Management, 18*(3), 246-268.

Djenouri, D., Khelladi, L., & Badache, N. (2005). A survey of security issues in mobile ad hoc networks. *IEEE communications surveys, 7*(4).

Erwin, C. (2008). Legal update: Living with the genetic information nondiscrimination act. *Genetics in Medicine, 10*(12), 869-873.

Faber, J., & Fonseca, L. M. (2014). How sample size influences research outcomes. *Dental press journal of orthodontics, 19*(4), 27-29.

Fei Yu, R. J. (2011). Mobile Device Security. Retrieved from Washington University in St. Louis Network Security website: http://www.cse.wustl.edu/~jain/cse571-11/ftp/mobiles.pdf

Fife-Schaw, C. (2014). Statistics Rules of Thumb for Violations of ANOVA Assumptions. Retrieved from http://www.surrey.ac.uk/psychology/current/statistics/

Fischer, S. H., David, D., Crotty, B. H., Dierks, M., & Safran, C. (2014). Acceptance and use of health information technology by community-dwelling elders. *International Journal of Medical Informatics, 83*(9), 624-635.

Flavián, C., & Guinalíu, M. (2006). Consumer trust, perceived security and privacy policy: three basic elements of loyalty to a web site. *Industrial Management & Data Systems, 106*(5), 601-620.

Fox, G., & Connolly, R. (2018). Mobile health technology adoption across generations: Narrowing the digital divide. *Information Systems Journal*.

Fung, B. (2013, 2013/12/20/). Security holes found in HealthCare.gov, Article. *The Washington Post*. Retrieved from https://www.washingtonpost.com/news/the-switch/wp/2013/10/30/healthcare-gov-had-a-glaring-security-flaw-that-wasnt-patched-until-last-week/?noredirect=on&utm_term=.4a2a7ab62e61

Gaff, B. M., Smedinghoff, T. J., & Sor, S. (2012). Privacy and Data Security. *Computer, 45*(3), 8-10.

Gaffney, K. (2009). Kiosks: Self-serve Patient Satisfaction. *Hayes Review*.

Gallagher, L. A. (2012). *Mobile Computing in Healthcare: Privacy and Security Considerations and Available Resources*. Paper presented at the Mobile Computing in Healthcare: Privacy and Security Considerations and Available Resources NIST/OCR Conference – June 6, 2012, HIMSS - USA. http://csrc.nist.gov/news_events/hiipaa_june2012/day1/day1-a1_lgallagher_mobile.pdf

Gambs, S., Killijian, M.-O., & del Prado Cortez, M. N. (2014). De-anonymization attack on geolocated data. *Journal of Computer and System Sciences, 80*(8), 1597-1614.

Gangwar, H., Date, H., Ramaswamy, R., Irani, Z., & Irani, Z. (2015). Understanding determinants of cloud computing adoption using an integrated TAM-TOE model. *Journal of Enterprise Information Management, 28*(1).

Garcia-Morales, V. J., Martín-Rojas, R., & Lardón-López, M. E. (2018). Influence of social media technologies on organizational performance through knowledge and innovation. *Baltic Journal of Management*.

Garg, V., & Camp, L. (2015). Risk Characteristics, Mental Models, and Perception of Security Risks.

Giunti, G., Giunta, D., Guisado-Fernandez, E., Bender, J., & Fernandez-Luque, L. (2018). A biopsy of Breast Cancer mobile applications: state of the practice review. *International Journal of Medical Informatics, 110*, 1-9.

Golden, B. (2009). The case against cloud computing, part one. *Retrieved April, 16*, 2011.

Gordon, W. J., Fairhall, A., & Landman, A. (2017). Threats to Information Security—Public Health Implications. *New England Journal of Medicine, 377*(8), 707-709.

Goswami, B., & Ravichandra, G. (2015). Public cloud user authentication and data confidentiality using image steganography with hash function. *American Journal of Applied Mathematics, 3*(1-2), 1-8.

Gozalvez, J. (2011). Mobile Traffic Expected to Grow More Than 30-Fold [Mobile Radio]. *Vehicular Technology Magazine, IEEE, 6*(3), 9-15.

Gribaudo, M., Iacono, M., & Marrone, S. (2015). Exploiting Bayesian Networks for the Analysis of Combined Attack Trees. *Electronic Notes in Theoretical Computer Science, 310*, 91-111.

Gross, R., & Acquisti, A. (2005). *Information revelation and privacy in online social networks.* Paper presented at the Proceedings of the 2005 ACM workshop on Privacy in the electronic society.

Grover, J., & Sharma, M. (2014). *Cloud computing and its security issues—A review.* Paper presented at the Computing, Communication and Networking Technologies (ICCCNT), 2014 International Conference on.

Grunin, G., Nachman, D. E., Nassar, N. M., & Nassar, T. M. (2015). Using Personalized URL for Advanced Login Security. In: US Patent 20,150,020,178.

Gunatilaka, D. (2011). A Survey of Privacy and Security Issues in Social Networks. Retrieved from Washington University St. Louis Network Security website: http://www.cse.wustl.edu/~jain/cse571-11/ftp/social.pdf

Günay, A., Erbuğ, Ç., Hekkert, P., & Herrera, N. R. (2014). Changing Paradigms in Our Interactions with Self-Service Kiosks. *Human-Computer Interfaces and Interactivity: Emergent Research and Applications: Emergent Research and Applications*, 14.

Gunter, T. D., & Terry, N. P. (2005). The emergence of national electronic health record architectures in the United States and Australia: models, costs, and questions. *Journal of Medical Internet Research, 7*(1).

Halevi, T., Memon, N., & Nov, O. (2015). Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks. *Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks (January 2, 2015)*.

Harman, L. B., Flite, C. A., & Bond, K. (2012). Electronic health records: privacy, confidentiality, and security. *The Virtual mentor, 14*(9), 712-719.

Harris, B., & Hunt, R. (1999). TCP/IP security threats and attack methods. *Computer Communications, 22*(10), 885-897.

He, S., Lee, G. M., & Whinston, A. B. (2014). Estimating the Treatment Effect of Spam Information Disclosure on Organizations: A Field Experiment.

HealthIT.gov. (2013). Healthcare Providers and Health Information Technology Infographic. Retrieved from https://www.healthit.gov/infographic/healthcare-providers-and-health-information-technology-infographic

Heinz, M. S. (2013). Exploring predictors of technology adoption among older adults.

HHS. (2013). Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; other modifications to the HIPAA rules. *Fed Regist, 78*(17), 5565-5702.

Holden, R. J., & Karsh, B.-T. (2010). The technology acceptance model: its past and its future in health care. *Journal of biomedical informatics, 43*(1), 159-172.

Householder, A., Houle, K., & Dougherty, C. (2002). Computer attack trends challenge Internet security. *Computer, 35*(4), 5-7.

Hsieh, C.-t. (2015). Implementing self-service technology to gain competitive advantages. *Communications of the IIMA, 5*(1), 9.

Hsieh, P.-J. (2015). Physicians' acceptance of electronic medical records exchange: An extension of the decomposed TPB model with institutional trust and perceived risk. *International Journal of Medical Informatics, 84*(1), 1-14.

Huang, K., Siegel, M., & Stuart, M. (2018). Systematically Understanding the Cyber Attack Business: A Survey. *ACM Computing Surveys (CSUR), 51*(4), 70.

Huber, M., Mulazzani, M., Weippl, E., Kitzler, G., & Goluch, S. (2011). Friend-in-the-middle attacks: Exploiting social networking sites for spam. *Internet Computing, IEEE, 15*(3), 28-34.

Huck, S. W., Cormier, W. H., & Bounds, W. G. (2000). *Reading statistics and research*: Harper & Row New York.

Hudson, K. L., Holohan, M., & Collins, F. S. (2008). Keeping pace with the times—the Genetic Information Nondiscrimination Act of 2008. *New England Journal of Medicine, 358*(25), 2661-2663.

Hunsaker, A., & Hargittai, E. (2018). A review of Internet use among older adults. *New Media & Society*, 1461444818787348.

Huntington, W., Covington, L., Center, P., Covington, L., & Manchikanti, L. (2011). Patient Protection and Affordable Care Act of 2010: Reforming the health care reform for the new decade. *Pain Physician, 14*(1), E35-E67.

Hydara, I., Sultan, A. B. M., Zulzalil, H., & Admodisastro, N. (2015). Current state of research on cross-site scripting (XSS)–A systematic literature review. *Information and Software Technology, 58*, 170-186.

Idowu, P. A. (2015). Information and Communication Technology: A Tool for Health Care Delivery in Nigeria. In *Computing in Research and Development in Africa* (pp. 59-79): Springer.

Ifrim, C., Pintilie, A.-M., Apostol, E., Dobre, C., & Pop, F. (2017). The art of advanced healthcare applications in big data and IoT systems. In *Advances in mobile cloud computing and big data in the 5G Era* (pp. 133-149): Springer.

Irani, D., Balduzzi, M., Balzarotti, D., Kirda, E., & Pu, C. (2011). Reverse social engineering attacks in online social networks. In *Detection of Intrusions and Malware, and Vulnerability Assessment* (pp. 55-74): Springer.

Jaege, T. (2013). Reference Monitor. 2013. Retrieved from http://ix.cs.uoregon.edu/~butler/teaching/10F/cis607/papers/jaeger-refmon.pdf

James, A., & Chung, J.-Y. (2015). Business and Industry Specific Cloud: Challenges and opportunities. *Future Generation Computer Systems*.

Jensen, M., Schwenk, J., Gruschka, N., & Iacono, L. L. (2009). *On technical security issues in cloud computing*. Paper presented at the Cloud Computing, 2009. CLOUD'09. IEEE International Conference on.

Jesdanun, A. (2004). April 8, 2004,"Boomers Closing Digital Divide", CBSNews. com. In: Associated Press.

Joshi, J. B., Aref, W. G., Ghafoor, A., & Spafford, E. H. (2001). Security models for web-based applications. *Communications of the ACM, 44*(2), 38-44.

Kafali, Ö., Jones, J., Petruso, M., Williams, L., & Singh, M. P. (2017). *How good is a security policy against real breaches?: a HIPAA case study*. Paper presented at the Proceedings of the 39th International Conference on Software Engineering.

Kalaiprasath, R., Elankavi, R., & Udayakumar, D. R. (2017). Cloud. Security and Compliance-A Semantic Approach in End to End Security. *International Journal Of Mechanical Engineering And Technology (Ijmet), 8*(5).

Kamerow, D. (2013). Regulating medical apps: which ones and how much? *BMJ, 347*.

Kassi-Lahlou, M., Mansour, J., & Michel, J.-C. (2014). Method for filtering packets coming from a communication network. In: Google Patents.

Kate, & Borten. (2010). Mobile Technology in Healthcare: Risks, Consequences & Remedies. *3M*.

Kaufman, L. M. (2009). Data security in the world of cloud computing. *Security & Privacy, IEEE, 7*(4), 61-64.

Kelley, P. G., Cranor, L. F., & Sadeh, N. (2013). Privacy as Part of the App Decision-Making Process (CMU-CyLab-13-003).

Kemper, G. (August 31, 2017). How Large Businesses Approach Cybersecurity in 2017: Survey. Retrieved from https://clutch.co/it-services/cybersecurity/resources/how-large-businesses-approach-cybersecurity-survey

Keselman, H., Rogan, J. C., Mendoza, J. L., & Breen, L. J. (1980). Testing the validity conditions of repeated measures F tests. *Psychological bulletin, 87*(3), 479.

Kevin. (2007). How much do medical records go for in the black market? Retrieved from http://www.kevinmd.com/blog/2007/01/how-much-do-medical-records-go-for-in.html

Kim, D. W., Yan, P., & Zhang, J. (2015). Detecting fake anti-virus software distribution webpages. *Computers & Security, 49*, 95-106.

Kizza, J. M. (2013a). Computer Network Vulnerabilities. In *Guide to Computer Network Security* (pp. 89-105): Springer.

Kizza, J. M. (2013b). Security Threats to Computer Networks. In *Guide to Computer Network Security* (pp. 63-88): Springer.

Knowles, B., & Hanson, V. L. (2018). Older Adults' Deployment of 'Distrust'. *ACM Transactions on Computer-Human Interaction (TOCHI), 25*(4), 21.

Kokkonen, E. W. J., Davis, S. A., Lin, H.-C., Dabade, T. S., Feldman, S. R., & Fleischer, A. B. (2013). Use of electronic medical records differs by specialty and office settings. *Journal of the American Medical Informatics Association, 20*(e1), e33-e38. doi:10.1136/amiajnl-2012-001609

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security, 64*, 122-134.

Kontaxis, G., Polakis, I., Ioannidis, S., & Markatos, E. P. (2011). *Detecting social network profile cloning*. Paper presented at the Pervasive Computing and Communications Workshops (PERCOM Workshops), 2011 IEEE International Conference on.

Kowitlawakul, Y., Chan, S. W. C., Pulcini, J., & Wang, W. (2015). Factors influencing nursing students' acceptance of electronic health records for nursing education (EHRNE) software program. *Nurse education today, 35*(1), 189-194.

Krishnamurthy, B., & Wills, C. E. (2008). *Characterizing privacy in online social networks*. Paper presented at the Proceedings of the first workshop on Online social networks.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2014). Advanced social engineering attacks. *Journal of Information Security and Applications*.

Krosnick, J. A. (2018). Questionnaire design. In *The Palgrave Handbook of Survey Research* (pp. 439-455): Springer.

Kumar, A. S., & Rani, D. U. (2014). PARADIGM SHIFT OF SOCIAL MEDIA MARKETING. *International Journal of Logistics & Supply Chain Management Perspectives, 2*(4), 421-425.

Kwon, J., & Johnson, M. E. (2013). Security practices and regulatory compliance in the healthcare industry. *Journal of the American Medical Informatics Association, 20*(1), 44-51.

Kwon, T., & Hong, J. (2015). Analysis and Improvement of a PIN-Entry Method Resilient to Shoulder-Surfing and Recording Attacks. *IEEE Transactions on Information Forensics and Security, 10*(2).

Lafuente, G. (2015). The big data security challenge. *Network Security, 2015*(1), 12-14.

Lent, K. J., Zelano, D. J., & Lane, S. (2013). Transformation of the Electronic Medical Record from Paper to Electronic: A Ground Theory.

Lepofsky, R. (2014). Web Application Vulnerabilities and the Damage They Can Cause. In *The Manager's Guide to Web Application Security:* (pp. 21-46): Springer.

Levin, K. A. (2005). Study design II. Issues of chance, bias, confounding and contamination. *Evidence-based dentistry, 6*(4), 102.

Lewis, C. J. (2014). *Cybersecurity in healthcare.* UTICA COLLEGE,

Li, C.-F. (2013). The Revised Technology Acceptance Model and the Impact of Individual Differences in Assessing Internet Banking Use in Taiwan. *International Journal of Business and Information, 8*(1).

Li, F., Zou, X., Liu, P., & Chen, J. (2011). New threats to health data privacy. *BMC bioinformatics, 12*(Suppl 12), S7.

Li, H., Gupta, A., Zhang, J., & Sarathy, R. (2014). Examining the decision to use standalone personal health record systems as a trust-enabled fair social contract. *Decision Support Systems, 57*, 376-386.

Li, J., Zhang, Y., Chen, X., & Xiang, Y. (2018). Secure attribute-based data sharing for resource-limited users in cloud computing. *Computers & Security, 72*, 1-12.

Lian, J.-W. (2015). Critical factors for cloud based e-invoice service adoption in Taiwan: An empirical study. *International Journal of Information Management, 35*(1), 98-109.

Lin, X., Featherman, M., Brooks, S. L., & Hajli, N. (2018). Exploring Gender Differences in Online Consumer Purchase Decision Making: An Online Product Presentation Perspective. *Information Systems Frontiers*, 1-15.

Lins, S., Schneider, S., & Sunyaev, A. (2018). Trust is good, control is better: Creating secure clouds by continuous auditing. *IEEE Transactions on Cloud Computing, 6*(3), 890-903.

Linthicum, D. (1999). Database-Oriented Middleware. Retrieved from http://www.information-management.com/issues/19991101/1560-1.html

Lwin, M., Wirtz, J., & Williams, J. D. (2007). Consumer online privacy concerns and responses: a power–responsibility equilibrium perspective. *Journal of the Academy of Marketing Science, 35*(4), 572-585.

Ma, H., & Wang, S. (2015). Development of Security WLAN Protocol Based on Quantum GHZ Stats. *Wireless Personal Communications, 80*(1), 193-202.

Mabo, T., Swar, B., & Aghili, S. (2018). *A Vulnerability Study of Mhealth Chronic Disease Management (CDM) Applications (apps).* Paper presented at the World Conference on Information Systems and Technologies.

Mahajan, H., & Giri, N. (2014). *Threats to Cloud Computing Security.* Paper presented at the VESIT, International Technological Conference-2014 (I-TechCON).

Maillet, É., Mathieu, L., & Sicotte, C. (2015). Modeling factors explaining the acceptance, actual use and satisfaction of nurses using an Electronic Patient Record in acute care settings: An extension of the UTAUT. *International Journal of Medical Informatics, 84*(1), 36-47.

Maji, A. K., Mukhoty, A., Majumdar, A. K., Mukhopadhyay, J., Sural, S., Paul, S., & Majumdar, B. (2008). *Security analysis and implementation of web-based telemedicine services with a four-tier architecture.* Paper presented at the Pervasive Computing Technologies for Healthcare, 2008. PervasiveHealth 2008. Second International Conference on.

Markelj, B., & Bernik, I. (2012). Mobile devices and corporate data security. *International Journal of Education and Information Technologies, 6*(1), 97-104.

Martínez-Pérez, B., De La Torre-Díez, I., & López-Coronado, M. (2015). Privacy and Security in Mobile Health Apps: A Review and Recommendations. *Journal of Medical Systems, 39*(1), 1-8.

May, A. (2013). healthcare.gov UNPLUGGED. (cover story). *Benefits Selling, 11*(12), 26-31.

Mazur, E., Signorella, M. L., & Hough, M. (2018). The Internet Behavior of Older Adults. In *Encyclopedia of Information Science and Technology, Fourth Edition* (pp. 7026-7035): IGI Global.

McDavid, J. (2012). HIPAA risk is contagious: practical tips to prevent breach. *The Journal of medical practice management: MPM, 29*(1), 53-55.

Meligy, A. M., Ibrahim, H. M., & Torky, M. F. (2015). A Framework for Detecting Cloning Attacks in OSN Based on a Novel Social Graph Topology.

Mell, P., & Grance, T. (2009). The NIST definition of cloud computing. *National Institute of Standards and Technology, 53*(6), 50.

Merete Hagen, J., Albrechtsen, E., & Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security, 16*(4), 377-397.

Merkow, M. S., & Breithaupt, J. (2014). *Information security: Principles and practices*: Pearson Education.

Mesbahi, M. R., Rahmani, A. M., & Hosseinzadeh, M. (2018). Reliability and high availability in cloud computing environments: a reference roadmap. *Human-centric Computing and Information Sciences, 8*(1), 20.

Mineraud, J., Mazhelis, O., Su, X., & Tarkoma, S. (2016). A gap analysis of Internet-of-Things platforms. *Computer Communications, 89*, 5-16.

Mishra, N., Sharma, T. K., Sharma, V., & Vimal, V. (2018). Secure Framework for Data Security in Cloud Computing. In *Soft Computing: Theories and Applications* (pp. 61-71): Springer.

Mittal, S., & Singh, A. (2014). A Study of Cyber Crime and Perpetration of Cyber Crime in India. *Evolving Issues Surrounding Technoethics and Society in the Digital Age*, 171.

Mitzner, T. L., Stuck, R., Hartley, J. Q., Beer, J. M., & Rogers, W. A. (2017). Acceptance of televideo technology by adults aging with a mobility impairment for health and wellness interventions. *Journal of Rehabilitation and Assistive Technologies Engineering, 4*, 2055668317692755.

Miyazaki, A. D., & Fernandez, A. (2001). Consumer perceptions of privacy and security risks for online shopping. *Journal of Consumer Affairs, 35*(1), 27-44.

Murphy, S. N., Gainer, V., Mendis, M., Churchill, S., & Kohane, I. (2011). Strategies for maintaining patient privacy in i2b2. *Journal of the American Medical Informatics Association, 18*(Suppl 1), i103-i108.

Mxoli, A., Gerber, M., & Mostert-Phipps, N. (2014). *Information security risk measures for Cloud-based personal health records.* Paper presented at the Information Society (i-Society), 2014 International Conference on.

Mxoli, A., Mostert-Phipps, N., & Gerber, M. (2017). *Information Security Risks Impacting Cloud-based Personal Health Records*. Paper presented at the The European Conference on Information Systems Management.

Nagin, D. S., & Weisburd, D. (2013). Evidence and Public Policy. *Criminology & Public Policy, 12*(4), 651-679.

Nazareth, D. L., & Choi, J. (2015). A system dynamics model for information security management. *Information & Management, 52*(1), 123-134.

networks, T. v. i. w. (2009, 2009/05/18/). Tackling vulnerabilities in wireless networks, Article. *New Straits Times*. Retrieved from http://go.galegroup.com/ps/i.do?id=GALE%7CA200163654&v=2.1&u=upitt_main&it=r&p=ITOF&sw=w

Neumann, P. G. (2015). Far-sighted thinking about deleterious computer-related events. *Communications of the ACM, 58*(2), 30-33.

O'Brien, D. G., & Yasnoff, W. A. (1999). Privacy, confidentiality, and security in information systems of state health agencies. *American journal of preventive medicine, 16*(4), 351.

O'Brien, R. G., & Kaiser, M. K. (1985). MANOVA method for analyzing repeated measures designs: an extensive primer. *Psychological bulletin, 97*(2), 316.

O'Brien, M. A., Olson, K. E., Charness, N., Czaja, S. J., Fisk, A. D., Rogers, W. A., & Sharit, J. (2008). Understanding technology usage in older adults. *Proceedings of the 6th International Society for Gerontechnology, Pisa, Italy*.

OCR. (2013). HIPAA & Breach Enforcement Statistics for October 2013 Retrieved from http://www.melamedia.com/v/Patient_Complaints.2003-2013.pdf

Oinas-Kukkonen, H., & Harjumaa, M. (2018). Persuasive systems design: key issues, process model and system features. In *Routledge Handbook of Policy Design* (pp. 105-123): Routledge.

Okazaki, S., Castañeda, J. A., Sanz, S., & Henseler, J. (2012). Factors affecting mobile diabetes monitoring adoption among physicians: questionnaire study and path model. *Journal of Medical Internet Research, 14*(6).

Or, C. K., Karsh, B.-T., Severtson, D. J., Burke, L. J., Brown, R. L., & Brennan, P. F. (2010). Factors affecting home care patients' acceptance of a web-based interactive self-management technology. *Journal of the American Medical Informatics Association*, jamia. 2010.007336.

Orebaugh, A., Ramirez, G., & Beale, J. (2006). *Wireshark & Ethereal network protocol analyzer toolkit*: Syngress.

Ortega Egea, J. M., & Román González, M. V. (2011). Explaining physicians' acceptance of EHCR systems: an extension of TAM with trust and risk factors. *Computers in Human Behavior, 27*(1), 319-332.

Oyelami, J. O., & Ithnin, N. B. (2015). Establishing a Sustainable Information Security Management Policies in Organization: A Guide to Information Security Management Practice (ISMP). *organization, 4*(01).

Paliwal, G., Mudgal, A. P., & Taterh, S. (2015). *A Study on Various Attacks of TCP/IP and Security Challenges in MANET Layer Architecture.* Paper presented at the Proceedings of Fourth International Conference on Soft Computing for Problem Solving.

Pan, X., Cao, Y., & Chen, Y. (2015). I Do Not Know What You Visited Last Summer: Protecting Users from Third-party Web Tracking with TrackingFree Browser.

Papageorgiou, A., Strigkos, M., Politou, E., Alepis, E., Solanas, A., & Patsakis, C. (2018). Security and privacy analysis of mobile health applications: The alarming state of practice. *IEEE Access, 6*, 9390-9403.

Pasquale, F., & Ragone, T. A. (2013). The Future of HIPAA in the Cloud.

Pasquale, F., & Ragone, T. A. (2014). PROTECTING HEALTH PRIVACY IN AN ERA OF BIG DATA PROCESSING AND CLOUD COMPUTING. *Stan. Tech. L. Rev., 17*, 595-595.

Pasquale, F. A., & Ragone, T. A. (2013). The Future of HIPAA in the Cloud. *Seton Hall Public Law Research Paper*(2298158).

Patton, M., Gross, E., Chinn, R., Forbis, S., Walker, L., & Chen, H. (2014). *Uninvited Connections: A Study of Vulnerable Devices on the Internet of Things (IoT).* Paper presented at the Intelligence and Security Informatics Conference (JISIC), 2014 IEEE Joint.

Paul III, D. P., Spence, N., & Bhardwa, N. (2018). Healthcare Facilities: Another Target for Ransomware Attacks.

Petersen, C., & DeMuro, P. (2015). Legal and Regulatory Considerations Associated with Use of Patient-Generated Health Data from Social Media and Mobile Health (mHealth) Devices. *Appl Clin Inform, 6*(1), 16-26.

Peterson, C., & Watzlaf, V. (2015). Telerehabilitation Store and Forward Applications: A Review of Applications and Privacy Considerations in Physical and Occupational Therapy Practice. *International Journal of Telerehabilitation, 6*(2), 75-84.

Porter, C. E., & Donthu, N. (2006). Using the technology acceptance model to explain how attitudes determine Internet usage: The role of perceived access barriers and demographics. *Journal of business research, 59*(9), 999-1007.

Potter, B. (2007). Mobile security risks: ever evolving. *Network Security, 2007*(8), 19-20. doi:10.1016/S1353-4858(07)70075-2

Pourhoseingholi, M. A., Baghestani, A. R., & Vahedi, M. (2012). How to control confounding effects by statistical analysis. *Gastroenterology and Hepatology from bed to bench, 5*(2), 79.

Provos, N., Friedl, M., & Honeyman, P. (2003). *Preventing privilege escalation.* Paper presented at the Proceedings of the 12th USENIX Security Symposium.

Ratchinsky, K. (2014). Top HIT trends for 2014: Accelerated change is coming. *Healthcare IT Newa*.

Rathi, A., & Parmar, N. (2015). *Secure Cloud Data Computing with Third Party Auditor Control.* Paper presented at the Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014.

Razali, N. M., & Wah, Y. B. (2011). Power comparisons of shapiro-wilk, kolmogorov-smirnov, lilliefors and anderson-darling tests. *Journal of Statistical Modeling and Analytics, 2*(1), 21-33.

Rebollo, O., Mellado, D., Fernández-Medina, E., & Mouratidis, H. (2015). Empirical evaluation of a cloud computing information security governance framework. *Information and Software Technology, 58*, 44-57.

Reddy, B. S. K., & Lakshmi, B. (2014). Enhanced Security Technique in WPA & WEP Based Wireless (Wi-Fi) Networks.

Reuters. (2014, September 25, 2014). On black market, medical records far more valuable than credit cards, Technology. *New York Post*. Retrieved from

http://nypost.com/2014/09/25/medical-records-far-more-valuable-than-credit-cards-to-hackers/

Rimal, B. P., Choi, E., & Lumb, I. (2009). *A taxonomy and survey of cloud computing systems.* Paper presented at the INC, IMS and IDC, 2009. NCM'09. Fifth International Joint Conference on.

Rindfleisch, T. C. (1997). Privacy, information technology, and health care. *Communications of the ACM, 40*(8), 92-100.

Rinehart-Thompson, L. A. (2013). *Introduction to Health Information Privacy and Security*: AHIMA Press.

Ritchey, R. W., & Ammann, P. (2000). *Using model checking to analyze network vulnerabilities.* Paper presented at the Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on.

Robertson, J. (2013, 4-6-14). Your Medical Records Are for Sale. Retrieved from http://www.businessweek.com/articles/2013-08-08/your-medical-records-are-for-sale

Rose, C. (2011). Smart phone, dumb security. *Review of Business Information Systems (RBIS), 16*(1), 21-26.

Russell, D., & Gangemi, G. (1991). *Computer security basics*: O'Reilly Media, Inc.

Ryan, J. (2014). Uncertain Future: Privacy and Security in Cloud Computing, The. *Santa Clara L. Rev., 54*, 497.

Rydstedt, G., Bursztein, E., Boneh, D., & Jackson, C. (2010). Busting frame busting: a study of clickjacking vulnerabilities at popular sites. *IEEE Oakland Web, 2*.

Sackett, D. L. (1997). *Evidence-based medicine.* Paper presented at the Seminars in perinatology.

Sametinger, J., Rozenblit, J., Lysecky, R., & Ott, P. (2015). Security challenges for medical devices. *Communications of the ACM, 58*(4), 74-82.

Sanatinia, A., & Noubir, G. (2015). OnionBots: Subverting Privacy Infrastructure for Cyber Attacks. *arXiv preprint arXiv:1501.03378*.

Sayed, B., Traore, I., & Abdelhalim, A. (2014). *Detection and mitigation of malicious JavaScript using information flow control.* Paper presented at the Privacy, Security and Trust (PST), 2014 Twelfth Annual International Conference on.

Schachat, A. P. (2003). What is HIPAA and what effect may it have on our journal? *Ophthalmology, 110*(6), 1074-1075.

Schmidt, K. (2018). Empowering users to understand their online privacy rights and choices through an interactive social media sign-up process.

Schofield, J. W. (2002). Increasing the generalizability of qualitative research. *The qualitative researcher's companion*, 171-203.

Schwingenschlögl, C., & Pilz, A. (2001). *Network Security at the Institute Level.* Paper presented at the EUNIS.

Sezgin, E., Yıldırım, S., Yıldırım, S. Ö., & Sumuer, E. (2018). *Current and Emerging mHealth Technologies: Adoption, Implementation, and Use*: Springer.

Shahriar, H., & Devendran, V. K. (2014). Classification of Clickjacking Attacks and Detection Techniques. *Information Security Journal: A Global Perspective, 23*(4-6), 137-147.

Shankar, R., & Duraisamy, S. (2018). Different Service Models and Deployment Models of Cloud Computing: Challenges.

Sharad, K., & Danezis, G. (2014). *An Automated Social Graph De-anonymization Technique.* Paper presented at the Proceedings of the 13th Workshop on Privacy in the Electronic Society.

Sharma, A., Harrington, R. A., McClellan, M. B., Turakhia, M. P., Eapen, Z. J., Steinhubl, S., . . . Chandross, K. J. (2018). Using Digital Health Technology to Better Generate Evidence and Deliver Evidence-Based Care. *Journal of the American College of Cardiology, 71*(23), 2680-2690.

Singhal, A., Winograd, T., & Scarfone, K. (2007). Guide to secure web services. *NIST Special Publication, 800*(95), 4.

Siponen, M., Pahnila, S., & Mahmood, A. (2007). *Employees' adherence to information security policies: an empirical study.* Paper presented at the IFIP International Information Security Conference.

Smith, A. (2014). Older Adults and Technology Use. *PewResearch Internet Project*.

Smith, B. (2008). Hacking the Kiosk. Retrieved from https://kioskindustry.org/wp-content/uploads/2016/02/wp-hacking-kiosk.pdf

Smith, G. (2012). White House Hacked In Cyber Attack That Used Spear-Phishing To Crack Unclassified Network. Retrieved from TECH website: http://www.huffingtonpost.com/2012/10/01/white-house-hacked-cyber-_n_1928646.html

Smith, G. S., & Futter, A. (2015). Management models for international cybercrime. *Journal of Financial Crime, 22*(1).

Solove, D. (2013). HIPAA Turns 10: Analyzing the Past, Present, and Future Impact.

Solove, D. J., & Hartzog, W. (2014). The FTC and Privacy and Security Duties for the Cloud.

Sood, A. K., & Enbody, R. (2011). Chain Exploitation—Social Networks Malware. *ISACA Journal, 1*, 31.

Sotto, L. J., Treacy, B. C., & McLellan, M. L. (2010). Privacy and Data Security Risks in Cloud Computing. *World Communications Regulation Report, 5*(2), 38.

Srinivasan, S. (2014). Risk management in the cloud and cloud outages. *Security, Trust and Regulatory Aspects of Cloud Computing in Business Environments*.

Srivastava, K., Awasthi, A. K., Kaul, S. D., & Mittal, R. (2015). A Hash Based Mutual RFID Tag Authentication Protocol in Telecare Medicine Information System. *Journal of Medical Systems, 39*(1), 1-5.

Steinbrook, R., & Sharfstein, J. M. (2012). The FDA Safety and Innovation ActThe FDA Safety and Innovation Act. *JAMA, 308*(14), 1437-1438.

Stone-Gross, B., Abman, R., Kemmerer, R. A., Kruegel, C., Steigerwald, D. G., & Vigna, G. (2011). The underground economy of fake antivirus software. *Economics of Information Security and Privacy III*, 55-78.

Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk management guide for information technology systems. *NIST Special Publication, 800*(30), 800-830.

Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications, 34*(1), 1-11.

Subhash, S. B. (2014). Data Confidentiality in Cloud Computing with Blowfish Algorithm. *International Journal of Emerging Trends in Science and Technology, 1*(01).

Sumra, I. A., Hasbullah, H. B., & AbManan, J.-l. B. (2015). Attacks on Security Goals (Confidentiality, Integrity, Availability) in VANET: A Survey. In *Vehicular Ad-hoc Networks for Smart Cities* (pp. 51-61): Springer.

Swanson, M. (2001). *Security self-assessment guide for information technology systems*. Retrieved from

Takyi, H., Watzlaf, V., MATTHEWS, J. T., Zhou, L., & DeAlmeida, D. (2017). Privacy and Security in Multi-User Health Kiosks. *International Journal of Telerehabilitation, 9*(1), 3.

Takyi, H., Watzlaf, V., Matthwes, J. T., Zhou, L., & DeAlmeida, D. (2017). Privacy and Security in Multi-User Health Kiosks. *International Journal of Telerehabilitation, 9*(1), 3.

Tung, F.-C., Chang, S.-C., & Chou, C.-M. (2008). An extension of trust and TAM model with IDT in the adoption of the electronic logistics information system in HIS in the medical industry. *International Journal of Medical Informatics, 77*(5), 324-335.

Turban, E., King, D., Lee, J. K., Liang, T.-P., & Turban, D. C. (2015). E-Commerce Security and Fraud Issues and Protections. In *Electronic Commerce* (pp. 459-520): Springer.

Uhley, P. (2006). Kiosk Security. Retrieved from http://www.defcon.org/images/defcon-14/dc-14-presentations/DC-14-Uhley.pdf

Usman, M., Jan, M. A., & He, X. (2017). Cryptography-based secure data storage and sharing using HEVC and public clouds. *Information Sciences, 387*, 90-102.

Van Royen, K., Poels, K., Daelemans, W., & Vandebosch, H. (2015). Automatic monitoring of cyberbullying on social networking sites: From technological feasibility to desirability. *Telematics and Informatics, 32*(1), 89-97.

van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior, 75*, 547-559.

van Vuuren, I. E., Kritzinger, E., & Mueller, C. (2015). *Identifying gaps in IT retail information security policy implementation processes.* Paper presented at the Information Security and Cyber Forensics (InfoSec), 2015 Second International Conference on.

Varghese, B., & Buyya, R. (2018). Next generation cloud computing: New trends and research directions. *Future Generation Computer Systems, 79*, 849-861.

Wang, C., Wang, Q., Ren, K., & Lou, W. (2010). *Privacy-preserving public auditing for data storage security in cloud computing.* Paper presented at the INFOCOM, 2010 Proceedings IEEE.

Wang, P., Zhang, X., & Huang, P. (2015). Privacy Preservation in Social Network Based on Anonymization Techniques.

Watson, H., & Rodrigues, R. (2018). Bringing privacy into the fold: Considerations for the use of social media in crisis management. *Journal of Contingencies and Crisis Management, 26*(1), 89-98.

Watzlaf, V. J., Moeini, S., & Firouzan, P. (2010). VoIP for telerehabilitation: A risk analysis for privacy, security, and HIPAA compliance. *International Journal of Telerehabilitation, 2*(2), 3--14.

Watzlaf, V. J., Moeini, S., Matusow, L., & Firouzan, P. (2011). VOIP for telerehabilitation: A risk analysis for privacy, security and HIPAA compliance: Part II. *International Journal of Telerehabilitation, 3*(1).

Watzlaf, V. R., & Ondich, B. (2012). VoIP for Telerehabilitation: A Pilot Usability Study for HIPAA Compliance. *International Journal of Telerehabilitation, 4*(1), 33-36.

Wei, L., Zhu, H., Cao, Z., Dong, X., Jia, W., Chen, Y., & Vasilakos, A. V. (2014). Security and privacy for storage and computation in cloud computing. *Information Sciences, 258*, 371-386.

Weinstein, R. S., Lopez, A. M., Joseph, B. A., Erps, K. A., Holcomb, M., Barker, G. P., & Krupinski, E. A. (2014). Telemedicine, telehealth, and mobile health applications that work: opportunities and barriers. *The American journal of medicine, 127*(3), 183-187.

White, J. M. (2008). *Family theories*: Sage.

Whitman, M. E., & Mattord, H. J. (2010). *Principles of information security*: Cengage Learning.

Wilkinson, G. (2018). General Data Protection Regulation: No silver bullet for small and medium-sized enterprises. *Journal of Payments Strategy & Systems, 12*(2), 139-149.

Wondracek, G., Holz, T., Kirda, E., & Kruegel, C. (2010). *A practical attack to de-anonymize social network users.* Paper presented at the Security and Privacy (SP), 2010 IEEE Symposium on.

Wu, S. S. (2007). *Guide to HIPAA Security and the Law*.

Yan, L., Rong, C., & Zhao, G. (2009). Strengthen cloud computing security with federal identity management using hierarchical identity-based cryptography. In *Cloud Computing* (pp. 167-177): Springer.

Yancey, A. K., Ortega, A. N., & Kumanyika, S. K. (2006). Effective recruitment and retention of minority research participants. *Annu. Rev. Public Health, 27*, 1-28.

Yang, H.-D., Lee, J., Park, C., & Lee, K. (2014). The Adoption of Mobile Self-Service Technologies: Effects of Availability in Alternative Media and Trust on the Relative Importance of Perceived Usefulness and Ease of Use. *International Journal of Smart Home, 8*(4).

Yang, K. C., Chye, G. N. S., Fern, J. C. S., & Kang, Y. (2015). Understanding the Adoption of Mobile Commerce in Singapore with the Technology Acceptance Model (TAM). In *Assessing the Different Roles of Marketing Theory and Practice in the Jaws of Economic Uncertainty* (pp. 211-215): Springer.

Yüksel, B., Küpçü, A., & Özkasap, Ö. (2017). Research issues for privacy and security of electronic health services. *Future Generation Computer Systems, 68*, 1-13.

Zhang, L., & Zhao, K. (2008). *Study on security of next generation network.* Paper presented at the Service Operations and Logistics, and Informatics, 2008. IEEE/SOLI 2008. IEEE International Conference on.

Zhang, Y., Chen, X., Li, J., Wong, D. S., Li, H., & You, I. (2017). Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing. *Information Sciences, 379*, 42-61.

Zhang, Y., & Paxson, V. (2000). *Detecting backdoors.* Paper presented at the Proc. of 9th USENIX Security Symposium.

Zhao, F., Gaw, S. D., Bender, N., & Levy, D. T. (2018). Exploring Cloud Computing Adoptions in Public Sectors: A Case Study. *GSTF Journal on Computing (JoC), 3*(1).

Zhao, J., Wang, L., Tao, J., Chen, J., Sun, W., Ranjan, R., . . . Georgakopoulos, D. (2014). A security framework in G-Hadoop for big data computing across distributed Cloud data centres. *Journal of Computer and System Sciences, 80*(5), 994-1007.

Zhou, B., & Pei, J. (2008). *Preserving privacy in social networks against neighborhood attacks.* Paper presented at the Data Engineering, 2008. ICDE 2008. IEEE 24th International Conference on.

Ziskovsky, T. (2017). 2017 HIPAA Breach Stats: Where Are We At? Retrieved from https://www.hipaaone.com/?s=2017+HIPAA+Breach