

2020

## Strategies to Lower Security Risks Involving Medical Devices in Patient Care

Brittany LaTonia Thigpen  
*Walden University*

Follow this and additional works at: <https://scholarworks.waldenu.edu/dissertations>



Part of the [Databases and Information Systems Commons](#)

---

This Dissertation is brought to you for free and open access by the Walden Dissertations and Doctoral Studies Collection at ScholarWorks. It has been accepted for inclusion in Walden Dissertations and Doctoral Studies by an authorized administrator of ScholarWorks. For more information, please contact [ScholarWorks@waldenu.edu](mailto:ScholarWorks@waldenu.edu).

# Walden University

College of Management and Technology

This is to certify that the doctoral study by

Brittany L. Thigpen

has been found to be complete and satisfactory in all respects,  
and that any and all revisions required by  
the review committee have been made.

## Review Committee

Dr. Charlie Shao, Committee Chairperson, Information Technology Faculty  
Dr. Steven Case, Committee Member, Information Technology Faculty  
Dr. Bob Duhainy, University Reviewer, Information Technology Faculty

Chief Academic Officer and Provost  
Sue Subocz, Ph.D.

Walden University  
2020

Abstract

Strategies to Lower Security Risks Involving Medical Devices in Patient Care

by

Brittany L. Thigpen

MS, Walden University, 2017

MS, University of South Alabama, 2013

BS, University of South Alabama, 2011

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

February 2020

## Abstract

Insufficient security and design strategies used during the analysis phase of medical device software development can lead to possible cybersecurity vulnerabilities with patient data. The purpose of this qualitative exploratory multiple case study was to explore strategies software developers use to implement security measures to protect patient information collected, sent, and stored by medical devices. The population for this study included software developers whose primary focus was on the security aspect of medical software in three software companies in the Baton Rouge, LA, area. The data collection process included semistructured interviews with 10 software developers and reviewing 16 organizational documents. The conceptual framework chosen for this study was the social shaping of technology, which aided in understanding how social, institutional, economic, and cultural factors affect technological decisions. An inductive analysis approach was used in this study to derive meanings and themes from participants experiences and triangulated with company documents to reach a comprehensive understanding of the research question. Prominent themes from data analysis included the security of medical device data, social influences on medical device security, establishing standard policies for medical device security, and factoring costs for medical device security. An implication for positive social change is that software developers who want to learn about similar issues and strategies to keep security breaches from happening in their organizations may be able to implement new strategies to limit cybersecurity vulnerabilities and the exposure of private personal health information.

Strategies to Lower Security Risks Involving Medical Devices in Patient Care

by

Brittany L. Thigpen

MS, Walden University, 2017

MS, University of South Alabama, 2013

BS, University of South Alabama, 2011

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

February 2020

## Dedication

I dedicate this work to my praying mother, Ruth, who continuously prayed for and with me through this journey. Thank you for all your love, support, and motivation throughout the years. I also want to dedicate this to my Uncle Charles, who passed away years ago. You were the reason I chose my initial research topic, medical devices to help those with disabilities, that was later molded into this study.

## Acknowledgments

First of all, I want to thank God for ordering my steps while I'm traveling on this journey called life. I want to recognize my committee chair, Dr. Charlie Shao, for the impromptu meetings while I was traveling for work, and also for your guidance, feedback, advice, and words of encouragement. Likewise, I would like to acknowledge my second committee member and URR, Dr. Steven Case and Dr. Bob Duhainy, for your suggestions, feedback, and support throughout this study. I cannot forget John and my sister Mandy, who were always willing to proofread whenever I asked. I would also like to thank the participants of this study who took time out of their busy schedules to partake in this research. Finally, I want to express gratitude to everyone who has shown support, expressed kind words, and motivated me to stay on this journey, from family, friends, colleagues, and classmates, thank you.

## Table of Contents

List of Tables .....	iv
List of Figures .....	v
Section 1: Foundation of the Study.....	1
Background of the Problem .....	1
Problem Statement .....	2
Purpose Statement.....	2
Nature of the Study .....	3
Research Question .....	4
Interview/Survey Questions.....	5
Demographic Questions.....	5
Interview Questions .....	5
Theoretical or Conceptual Framework .....	6
Definition of Terms.....	7
Assumptions, Limitations, and Delimitations.....	8
Assumptions.....	8
Limitations .....	8
Delimitations.....	9
Significance of the Study .....	9
Contribution to Information Technology Practice .....	9
Implications for Social Change.....	10
A Review of the Professional and Academic Literature.....	11



The Social Shaping of Technology .....	13
Medical Device Usage in Healthcare .....	21
Risks Involved with Medical Devices .....	28
SST Influences on Security Strategies .....	36
Transition and Summary .....	52
Section 2: The Project .....	54
Purpose Statement .....	54
Role of the Researcher .....	54
Participants .....	58
Population and Sampling .....	60
Ethical Research .....	64
Data Collection .....	66
Instruments .....	66
Data Collection Technique .....	70
Data Organization Techniques .....	73
Data Analysis Technique .....	75
Reliability and Validity .....	78
Reliability .....	79
Research Method and Design .....	81
Research Method .....	82
Research Design .....	84
Strategies for Trustworthiness .....	86

Transition and Summary .....	89
Section 3: Application to Professional Practice and Implications for Change .....	91
Overview of Study .....	91
Presentation of the Findings.....	91
Theme 1: Securing Medical Device Data .....	94
Theme 2: Social Influences on Medical Device Security .....	101
Theme 3: Establishing Standard Policies for Medical Device Security .....	107
Theme 4: Factoring Costs for Medical Device Security.....	113
Applications to Professional Practice .....	120
Implications for Social Change.....	122
Recommendations for Action .....	124
Recommendations for Further Study .....	125
Reflections .....	127
Summary and Study Conclusions .....	128
References.....	129
Appendix A: Human Research Participants Certificate of Completion .....	168
Appendix B: Interview Protocol .....	169

## List of Tables

Table 1 Themes for Extensive Collaboration is Critical.....	94
Table 2 Frequency of First Major Theme .....	95
Table 3 Frequency of Second Major Theme.....	102
Table 4 Frequency of Third Major Theme .....	108
Table 5 Frequency of Fourth Major Theme.....	113

## List of Figures

Figure 1. Common types of medical devices used in healthcare .....	22
Figure 2. Wireless communication components between medical devices and healthcare providers. ....	26

## Section 1: Foundation of the Study

### **Background of the Problem**

Medical devices are used by healthcare professionals to perform many tasks such as accessing critical patient information, making an accurate diagnosis quickly, improving patient-doctor communication, and providing remote patient monitoring (Ventola, 2014). The increasing rate of chronic and customary conditions requiring continuous patient monitoring leads to an increase in the cost of healthcare use in the United States (Klersy et al., 2016). These devices are used in healthcare to improve the lives of patients while advancing the services provided (Azhar et al., 2016). Patients who require intensive medical service often receive services from multiple providers, that is, live-in care, specialty care, personal care, and so forth, to receive the needed round-the-clock attention (Agency for Healthcare and Quality, 2012). To reduce the need of seeing patients for routine care, medical professionals are leaning towards the use of medical devices to collect data to aid in healthcare assessments (Klonoff, 2015).

For medical devices to work properly, these devices must connect via computer networks, which could lead to possible cybersecurity vulnerabilities (Williams & Woodward, 2015). Healthcare providers choose to use medical devices in order to add to a patient's quality-of-life. However, the security and vulnerabilities associated with these devices are a major concern. Klonoff (2015) mentioned that if a security threat occurred, there could be an issue with the accuracy of information found on the device as well as problems completing the device-designed tasks. If the device is hacked, sensitive personal information, such as a user's name or social security number, could be leaked.

Additionally, if these devices can be hacked, there is an increased risk of malware vulnerabilities. Software developers in the healthcare industry and officials of the U.S. Food and Drug Administration (FDA) are aware of malware occurrence in medical devices and must develop strategies to limit security threats in order to protect information as well as information systems (FDA, 2015b).

### **Problem Statement**

The usage of medical devices in healthcare is often vulnerable to security breaches when connected to the internet, hospital networks, and to other medical devices (FDA, 2016). Williams and Woodward (2015) reported that a cyberattack on medical devices and its infrastructures have occurred in 94% of healthcare organizations. The general IT problem is that security risks and threats are found when data is collected, sent, and stored using medical devices in patient healthcare. The specific IT problem is that some software developers lack strategies to implement security measures to protect sensitive patient information collected, sent, and stored by medical devices.

### **Purpose Statement**

The purpose of this qualitative exploratory multiple case study was to explore strategies software developers use to implement security measures to protect patient information collected, sent, and stored by medical devices. The population for this study included software developers whose primary focus is on the security aspect of medical software in three software companies in the Baton Rouge, LA, area. The software developers participated in open-ended interviews to discuss strategies for securing software in medical devices. I also reviewed company documents to gather additional

information on security strategies to triangulate the data. The implications for positive social change are that new strategies may limit the exposure of private personal health information (PHI) from unauthorized users.

### **Nature of the Study**

For this study, I used a qualitative approach to help explore strategies for implementing security measures on medical devices. Qualitative research is used to investigate a problem with contextual information about the underlying reasons, opinions, and motivations (O'Cathain, Thomas, Drabble, Rudolph, & Hewison, 2013). The qualitative research methods make use of focus groups, interviews, and the review of documents to collect data and discover themes that would be beneficial to the research (Mikkonen, Elo, Kuivila, Tuomikoski, & Kaariainen, 2016). I used the qualitative method because the purpose of this study was to seek contextual information about strategies for implementing security measures for medical devices. Quantitative research is used when statistics will be applied to numerical-based data to quantify a problem (Hoe & Hoare, 2013). I did not use the quantitative method in this study because I was not quantifying information. Mixed-methods research is a combination of both quantitative and qualitative methods used to examine a problem (Kamalodeen & Jameson-Charles, 2016). I did not select the mixed-method approach because I did not use the quantitative method. To further the investigation into trends using a qualitative approach, I considered various approaches to properly explore security strategies (O'Cathain et al., 2013).

Several approaches can be used to conduct a qualitative research study; they include case studies, grounded theory, phenomenological, narrative, and ethnographic designs (Hyett, Kenny, & Dickson-Swift, 2014). After reviewing these five qualitative approaches to inquiry, the three approaches that are most appropriate for an IT problem are phenomenology, ethnography, and case study (Elkatawneh, 2016).

Phenomenological research involves a researcher interpreting common meanings from several individuals' lived experiences (Hyett et al., 2014). I did not select

phenomenological research because this study was not focused on lived experience.

Ethnographic research involves a researcher interpreting and describing shared and learned patterns of behaviors, beliefs, and values by immersing in the culture as an active participant (Baskerville & Myers, 2015). I did not select the ethnographic research design because this study was not based on cultural experience as a participant. A case study design is used when a researcher wants to study a specific phenomenon, understand how decisions were made over a time frame for similar cases, and capture unique information on the subject (Tsang, 2014). To best align with the focus of this study, a case study was the best design choice to explore the strategies to secure data collected on medical devices.

### **Research Question**

RQ: What are strategies that software developers use to implement security measures to protect sensitive patient information collected, sent, and stored on medical devices?



## **Interview/Survey Questions**

The open-ended interview questions follow:

### **Demographic Questions**

1. What is your primary role in the organization in regards to medical devices?
2. How long have you been working with the software for medical devices?
3. What are issues that occur when creating/updating software for medical devices? How are those issues mitigated?
4. How is medical device security handled in your organization?
5. How knowledgeable are you with the interrelation of cloud security and medical devices?
6. Is there a team that focuses directly on the security aspect of medical devices?  
If so, what is their role?
7. What are the different types of medical devices software created in your organization?

### **Interview Questions**

1. What are design choices used for creating the software for these medical devices?
2. How do security policies in your organization and/or outside federal regulations affect how the software for medical devices is created?
3. How do users and hackers affect how the software for medical devices is created (i.e., prevent jailbreaking)?

4. Do budgets for healthcare data security affect security choices for medical devices?
5. Are there any social influences (i.e., user acceptance) that affect how the software is developed?
6. With technology always changing, what strategies do software developers in your organization use to keep the software in older medical devices compatible with new security measures?
7. Is there any additional information you can provide on how medical device security strategies are influenced by internal or external influences?

### **Conceptual Framework**

The conceptual framework chosen for this study is the social shaping of technology (SST). MacKenzie and Wajcman (1999) developed the SST in 1985 to understand how social, institutional, economic, and cultural factors affect technological decisions. A common misconception, addressed by the authors of this theory, is that technology is shaped based on how users and developers influence the success or failure of information and communication technologies, such as by not using systems in the way they were intended to be used (MacKenzie & Wajcman, 1999). However, Noble (1984) stated that technology has a twofold existence, one which complies with the goals of designers and interests of power, and another that contradicts them by revealing unintended results and unexpected outcomes after being finalized.

Instead of concentrating on the impacts technology has on society, SST focuses on the influences society has on technology. With cyberattacks happening in over 90%

of healthcare organizations in the United States, software developers are faced with a “fork in the road” approach. This approach allows software developers to make a choice between various security routes that could potentially lead to different technological outcomes. I utilized SST in this study to explore how the influences society has on technological advances impact software developers’ strategies for implementing security measures on medical devices. Additionally, I utilized SST to identify how social, institutional, economic and cultural factors may influence the direction of innovation, the practices used by software developers, and the outcomes of technological decisions based on external factors. This framework aligned with medical device security and aided in interpreting and understanding how hackers, technology advances, and patient/doctor usage of these devices for data transmission influence the decisions of software developers.

### **Definition of Terms**

*Personal health information:* PHI includes any kind of information, such as medical history, demographic information, lab and testing results, insurance information, and so forth, that can be used to identify an individual and their corresponding care (Gloyd, Wagenaar, Woelk, & Kalibala, 2016).

*Remote patient monitoring:* Remote patient monitoring is a technology that allows healthcare providers to surveil patients outside of ordinary clinical settings (e.g., in the home), which may increase patient care and lower healthcare costs (Giger et al., 2015).

*Agnosticism:* Agnosticism is having an unbiased view on human or nonhuman actors affecting technology changes (Christiansen & Gasparin, 2016).

*Generalized symmetry:* Generalized symmetry is a uniformed term to explain conflicting views between human or nonhuman actors (Dumay & Rooney, 2016).

*Free association:* Free association requires that all previous distinctions of social, cultural, or natural impacts of technology are eliminated to counteract bias towards human or nonhuman actors (Dumay & Rooney, 2016).

### **Assumptions, Limitations, and Delimitations**

#### **Assumptions**

Assumptions made in research are the topics of the subject that the researcher assumes to be true (Massis & Kotlar, 2014). For the study, three assumptions were made. First, I assumed the interviewed developers would have a minimum of 2 or more years of experience in the security aspect of the software developed for the medical field. Secondly, I assumed all of the participants would not have the same level of experience and knowledge on the topic of security strategies to protect sensitive patient information collected, sent, and stored by medical devices. Thirdly, I assumed all participants would answer interview questions accurately and honestly to ensure the integrity of information gathered.

#### **Limitations**

In research, sometimes limitations arise that are out of the control of the researcher (Hyett et al., 2014). Limitations are the weaknesses found in the study that could have an adverse effect on the decisions made or the outcome of the study (Hyett et al., 2014). One limitation of this study was whether or not the participants answer some questions using personal bias. When researching and making decisions, a researcher

must not exhibit confirmation bias, which means only acknowledging information that confirms prior belief (Denscombe, 2014). For software developers interviewing for the same company, interview questions can be shared, which could negatively affect the validity and integrity of the interview responses. Additionally, if a developer did not have a well-rounded experience through the lifecycle of creating secure software, such as, an understanding of federal regulations or organizational policies, the developer may not be able to answer all questions. Finally, there may have been some questions that the participants could not answer, or they may have altered their responses due to HIPAA laws and/or the organization's information security procedures.

### **Delimitations**

Delimitations set the scope of research, which outlines the boundaries of what the researcher intends to study (Svensson & Doumas, 2013). The delimitations of this study included only allowing participants who have 2 or more years of experience working with the security aspect of the software. In addition, selected participants must have currently worked in developing the software used to make these devices secure. Furthermore, the interview questions and any information gathered was directly related to the strategies to implement security measures.

### **Significance of the Study**

#### **Contribution to Information Technology Practice**

This study may contribute to IT practice by providing strategies to secure patient information collected, sent, and stored on medical devices. Numerous healthcare providers are using medical devices as a new way of examining patients' data without

physically seeing patients. The benefits of using medical devices include reductions of doctor visits, round-the-clock monitoring, and less-evasive surgeries. However, threats towards cybersecurity could expose data to unauthorized users, which would be disastrous for patients, doctors, and software developers. Researchers at the FDA stated that cybersecurity vulnerabilities could be found at any moment if a glitch or security flaws are exposed in the software (FDA, 2015a). Vulnerabilities are problematic because they are hard to detect and could provide hackers with the source to spread malware in the devices. Any task conducted by these devices must be secured across a network for both patients and healthcare providers due to shared data. Software developers who want to learn about similar issues and strategies to keep security breaches from happening in other organizations could use this study as a basis to understand suggested security strategies for securing mobile devices. Strategies in security measures for these devices would allow software developers to ensure vulnerability decreases.

### **Implications for Social Change**

The implication for positive social change is that software developers may use new strategies to limit the exposure of private PHI from unauthorized users. Software developers' decision to use new security strategies can have a snowball effect on how users and healthcare providers view and use medical devices. Enhanced strategies for data security may also increase a user's willingness to trust, use, and rely on medical devices. Furthermore, increased usage of medical devices will improve the efficiency of healthcare providers practices and help patients live longer, healthier, and more productive lives (Nakrem, Solbjor, Pettersen, & Kleiven, 2018). Security attacks on

medical devices can lead to lawsuits, profit loss, recovery costs, and fines. Adverse results due to a breach in security are the main reasons why learning preventative measures to keep these devices secure is necessary. Healthcare providers invest considerable amounts of time and money to enhance security procedures on medical devices (FDA, 2015b). Enhanced security measures will lead to a change in how healthcare providers and patients use and manage the devices. Reducing the occurrence of security threats to these devices will ensure that sensitive patient information is properly managed using medical devices.

### **A Review of the Professional and Academic Literature**

The purpose of this qualitative exploratory multiple case study was to explore strategies software developers use to implement security measures to protect patient information collected, sent, and stored by medical devices. The focus of the literature review was the research question: What are strategies that software developers use to implement security measures to protect sensitive patient information collected, sent, and stored on medical devices? Throughout the process of the literature review, collected content was organized according to established themes while keeping social influences on technology and security strategies for medical device software in mind. First, the conceptual framework, SST is explored. Next, the current usage of both medical devices and the internet of things (IoT) in healthcare, along with privacy and security challenges, are examined. Then, I explore strategies used by software developers to secure the data collected, sent, and stored by medical devices. Finally, SST is investigated to discover how the influences society has on technological advances impact software developers'

strategies for implementing security measures on medical devices. By exploring the SST conceptual framework, software developers can gain an understanding of the history, usage, and the modifications made by other researchers to form other theories since the conception of the SST theory. Understanding the different strategies that are either still active, inactive, or modified shows how technological advances in medical devices affect strategies for security.

To gather the information needed to conduct this literature review, 163 articles, journals, and government websites were referenced. The search terms for the resources included *cyberattacks on medical devices*, *social shaping of technology usage*, and *healthcare mobile technology security measures*. A majority of the references were obtained from multiple databases and libraries including the Walden Library, Google Scholar, ProQuest Computing, ACM Digital Library, and IEEE Xplore Digital Library. Using Ulrich's Global Serials Directory and various journal websites, I was able to identify whether the collected references were peer-reviewed. Out of 163 articles, 153 (93%) were peer-reviewed, and 147 (90%) were published within 5 years of my anticipated graduation date.

The literature focused on four key areas: (a) privacy and security challenges in the wireless data transmission, (b) risks involved with using medical devices, (c) strategies to enhance medical device safety, and (d) the four influences on medical device security based on the SST theory. Influences include the social, institutional, cultural, and economic factors of SST as it correlates with technological design choices that influence



the direction of innovation, the practices used by software developers, and the outcomes of technical decisions based on external factors.

### **The Social Shaping of Technology**

Researchers have been asking for years what affects the kind of technology produced. Researchers in opposition to the notion that technology is not influenced by any social or human influences have looked for theories to aid in understanding the progression of technology. Researchers such as Oguz (2016) undertook studies to understand the relationship between outside stimulus and the decision-making process associated with technology changes. Some researchers have a technological determinism point-of-view, which means that changes in technology are independent of any form of social influences, and in fact, have a direct impact on society (Thompson, 2016; Papageorgiou, & Michaelides, 2016). In opposition, MacKenzie and Wajcman (1999) created SST to illustrate how technological advancement, execution, and use are affected by social factors such as culture and economics. Using the SST approach, researchers are given a set of theoretical tools that can be utilized to break down the development of technologies in the healthcare industry (Vanniere, Guilyardi, Toniazzo, Madec, & Woolnough, 2014). The SST approach goes beyond conventional methodologies researchers use to examine the effects of innovations, and it places a focus on the way that particular technology is impacted by outside influences. In other words, using the SST method, researchers can examine the influences that shape technology.

Williams and Edge (1996) elaborated on MacKenzie and Wajcman's (1999) theory by emphasizing how social factors impact the direction, speed, type, practices, and

outcomes of technological changes. Pronovost, Powers, and Jin (2017) described how vendors in healthcare technology modify their software based on the input on problems, wants, and needs of stakeholders and users to improve software needs in patient care. Pronovost et al. (2017) and Shahmarichatghieh, Harkonen, Haapasalo, and Tolonen (2016) deliberated on how a technology development model would increase vendor collaborations by considering market demands and other influences that would further enhance healthcare technology. Researchers like Shahmarichatghieh et al. (2016) speculated that the technology development lifecycle is initially developed based on applicable ideas but is later transformed as a result of market usage statistics. To handle the evolution of technology, researchers continue to create or modify existing theories to correlate with the changes in technology.

**Changes in the theory.** With disagreements behind the specific cause of technological changes, the SST theory has been both criticized and modified since its beginning. From its creation, SST characterization was formed by two contradictory viewpoints; technological determinism, in which technology affects social change (Thompson, 2016), and social and economic determinism, in which social and economic factors influence the direct development and use of technology (O’Riordan & O’Connell, 2014). The needs of consumers, perceptions of security threats, and social conditions are some reasons why developers brought forth new technologies based on institutional pressures (Gopalakrishna-Remani, Jones, & Camp, 2018). With many changes in technology since 1985, researchers needed to enhance and modify this theory to comprehend the complex growth in technology. Researchers such as Mackey and

Gillespie (1992) believed that the SST approach to the relationship between society and technology should be extended. Theories created that supported the extension of the SST include the social construction of technology (SCOT), which underlines interpretive adaptability and significant actors in technological changes; and the actor-network theory (ANT), which is used by researchers to manage networks, interpretation, and irreversibility in technological changes (Bijker, Hughes, Pinch, & Douglas, 2012).

**Supportive theories.** The SST theory was developed to aid researchers in understanding if the advancement of technology changes were independent of influences or reliant on societal impacts (Graham & Choi, 2016). MacKenzie and Wajcman (1999) developed this theory due to the belief that there was a different perspective on technological changes outside of technological, social, and economic determinism (Kikuchi, 2016; Stetsenko, 2016). Some of the researchers who developed theories in support of SST believed that the motivation behind the outcome of technology innovation is based on human influences instead of social influences (Graham & Choi, 2016; Stetsenko, 2016; Thompson, 2016).

The ANT focused on deriving the factors of social influences in technological changes, removing those social forces, and treating the remaining factors and objects as actors in technology changes (Bilodeau & Potvin, 2016). Bijker et al. (2012) developed SCOT with the belief that technological enhancements cannot happen without first understanding how that technology is used and interpreted by critical stakeholders (Kerschner & Ehlers, 2016). The SST, ANT, and SCOT theories all focus on how

external factors affect the advancement of technology. However, each theory is used by researchers to conceptualize the factors differently.

**Contrasting theories.** ANT and SCOT are similar to SST in the belief that there are external forces outside of the technology itself that influence change. While SST breaks down the different kinds of influences, researchers using ANT view nonhuman and human agents, also known as actors, equally when analyzing factors that influence technology (Booth, Andrusyszyn, Iwasiw, Donelle, & Compeau, 2016). Using the three principles found in ANT, agnosticism, generalized symmetry, and free association, a distinction cannot be made between the social, natural, or technological influences (Dumay & Rooney, 2016; Mills, 2017; Christiansen & Gasparin, 2016). SCOT focuses on defining a problem before determining a solution by identifying and assessing social groups based on the market, the user types, and how the technology is being used (Madsen, Brown, Elle, & Mikkelsen, 2017). In comparison to SST, SCOT takes more into account on how to innovate technology based on human needs in order to keep the technology relevant.

The diffusion of innovations (DOI) theoretical framework is used by researchers to focus on the social processes that affect the acceptance or rejection rates of fully formed technology based on cultural influences (Cracchiolo, Roman, Kutler, Kuhel, & Cohen, 2016). Researchers use the DOI theory to determine how social criteria affect adopters and the decision-making process of an innovation (Bianchi, Di Benedetto, A., Franzo, & Frattini, 2017; Cracchiolo et al., 2016). On the other hand, researchers often push the significance of focusing on the diversity of technology rather than the social

criteria. Focusing on the diversity of technology while ignoring the social areas that affect technology changes is irrational (Vanniere et al., 2014; Cram, Proudfoot, & D'Arcy, 2017). Examining how various factors and influences have transformed technological designs will attest to the importance of evaluating both the diversity of technology as well as the social criteria.

**SST and IT practice.** When software developers create or make enhancements to technology, they often attempt to govern how the technology is used. However, software developers cannot determine how the users will see or interpret the new technology. Therefore, collaboration amongst software developers, business leaders, and stakeholders is essential (Martins & Zacarias, 2017). Newer technology is affected more by social factors than older technology because user adoption and usage are not yet established (Sabi, Uzoka, Langmia, & Njeh, 2016). SST has been used in IT to understand technological changes based on the external intersecting trends outside of technology. SST was used by researcher Kikuchi (2016) to examine how social and organizational factors affected the development and operations of the bullet train. SST was also used by Rennkamp and Bhuyan (2016) to present how institutional influences, consisting mainly of government departments, agencies, state-owned enterprises, and private businesses, caused the government in South Africa to choose a nuclear energy program despite the ample access to fossil and renewable energy resources.

With the increasing capabilities and features in mobile devices, some users attempt to hack or modify their devices to have more functionality. Lee and Soon (2017) examined Apple's earlier opposition towards consumer-driven innovation, which took

place in the form of jailbreaking. Social shaping of Apple's smartphone technology has taken place since the initial launch of the iPhone. Initially only having preinstalled apps to use, Apple developed the App Store to leverage the consumers' want of third-party apps (Lee & Soon, 2017). Taylor and Levin (2014) discussed how later upgrades to Apple devices were due to social influences, such as Apple users wanting Android-like features. The objective of smartphone manufacturers is to enhance the innovation of their products and to increase user adoption (Jung, Kim, & Choi, 2016; Taylor & Levin, 2014). Both Apple and Samsung are two examples of companies that will take measures to increase user satisfaction even if the increase means producing similar products as their rivals to achieve user interest.

Likewise, researchers in the automobile industry found that modification to the technology in vehicles was a direct effect of the social influences on technology. The added functionality to the various makes and models of vehicles is driven by user interest, safety demands, and costs. When automobiles were first created, the owners usually did not find out about problems until something went drastically wrong. Computer diagnostics were later introduced as a way to point out potential problems before any real damage occurred (Mellit, Tina, & Kalogirou, 2018). All-wheel drive is another feature that was introduced to help drivers have more control of their vehicles when driving over unsafe roadways (Ni & Hu, 2017). Once upon a time, having a radio with a cd and/or cassette player was known as a pristine luxury for automobiles; today, users search for cars that offer upgrades such as remote start, satellite radio, full entertainment systems to watch movies, built-in GPS, Bluetooth capabilities, Wi-fi, and

so forth. Enhancements in-vehicle technology to meet consumer wants allows the software to be susceptible to potential cyberattacks (Pugnetti & Schlapfer, 2018).

Throughout the history of innovative automobile transformation, the common reason for these changes in the technology found in automobiles was directly associated with either the social, cultural, economic, or institutional influences that automobile manufacturers needed to take into account (Coppola & Morisio, 2016).

Keeping up with changes in technology, the quality of customer care, and customer experience are only some of the guidelines that manufacturers should consider when designing and marketing products (Coppola & Morisio, 2016; Brand, 2017; Vanniere et al., 2014). The time and money spent by companies' stakeholders to ensure that their products are matching or exceeding those of their rivals, existing technology, user expectations, and other factors follow the SST principles on how outside factors influences technology (MacKenzie & Wajcman, 1999). Kodak was a company that once dominated the photography industry. However, internal stakeholders in Kodak did not consider the innovative changes the digital market brought that would later shape the photography industry, thus, getting left behind in the introduction of digital technology (San Cornelio & Gomez Cruz, 2014). The list of innovative changes that are influenced by social or human influences will continue to grow as shareholders realize the importance of not excluding outside impacts in decision-making strategies (San Cornelio & Gomez Cruz, 2014; Thompson, 2016).

Previous researchers have applied variations of the SST as a conceptual framework to understand changes in technology outside of the typical "black box"

viewpoint. The “black box” viewpoint shows influences as the stimuli and new technology as the response, but this view does not disclose what goes on to shift from the stimuli to the response (Kraft & Bausch, 2016). With the increased use of technology in healthcare, researchers are seeking to find what goes on in the box itself. Pesapane, Volonte, Codari, and Sardanelli (2018) noted how legal issues such as healthcare regulatory requirements, ethical approvals, and adherence to different policies affected the expansion of using mobile phones as medical devices. Along with regulatory processes, Allenby et al. (2018) discussed how clinical investigations on medical devices influence the premarket evaluation and the prediction of success once the devices are on the market. This paper will build on SST by understanding and discussing the strategies software developers use that are encouraged or discouraged by different external factors. Influences such as user modifications; attacks on medical devices by unauthorized third parties; misuse by consumers; attacks on medical networks; and federal regulations, all affect the strategies software developers use to secure medical devices (Sametinger, Rozenblit, Lysecky, & Ott, 2015; Williams & Woodward, 2015). Consequently, software developers and other stakeholders are highly interested in continually finding new ways to protect the security of medical devices.

The theory selected for the conceptual framework for this study was selected based on multiple factors, beginning with how the research question would be analyzed. Using the SST as the conceptual lens assisted in understanding how society influenced the security strategies developers of medical devices. Additionally, analyzing current security measures expanded on different points of views on how software developers

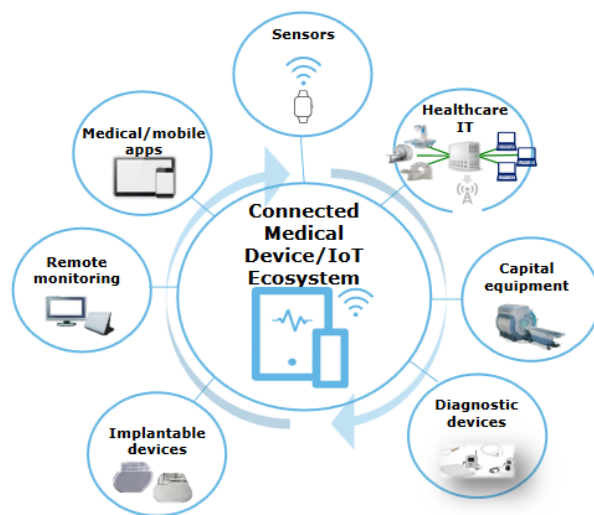


should handle security concerns. The goal of this study was to explore strategies used by software developers to secure and protect sensitive information collected, sent, and stored using medical devices. Stakeholders and users of various medical devices that work over a network, such as insulin pumps, defibrillators, or pacemakers, called for research to increase protection on these devices (Stine, Rice, Dunlap, & Pecarina, 2017). To mitigate increasing attacks, software developers must understand the usage of these devices. However, to address the security strategies of medical devices, an understanding of how these medical devices are used, privacy and security challenges that are currently found, and security measures involved needed to be investigated first.

### **Medical Device Usage in Healthcare**

Medical devices are used to prevent, diagnose, cure, treat, or monitor diseases and other health conditions under the supervision of healthcare providers (Khan, Ostfeld, Lochner, Pierre, & Arias, 2016). Medical devices can be either worn or implanted and consist of multiple sensors, processors, and microcontrollers to monitor and aid with various healthcare treatments (Haghi, Thurow, & Stoll, 2017). Yearly, there are hundreds of thousands of medical devices issued to patients. Four years prior to the study conducted by Doyle, Gurses, and Pronovost (2017), the number of non-disposable medical devices used in healthcare grew 23%. These devices routinely collect and send sensitive data, hence the reason adequate software, correct permissions, and top-of-the-line security measures must be in place to ensure the privacy and security of medical information (Grindrod et al., 2017). Even though these devices are wirelessly connected, each medical device is interconnected and contains embedded computer systems that

handle operations. Figure 1 has a list of the common types of medical devices used in healthcare systems.



*Figure 1.* Common types of medical devices used in healthcare. Reprinted from *Managing Business Partner Risks in a Cloud and IoT Universe* (p. 17), by A. Sood, A. Sethi, & D. Messerschmidt, 2017, retrieved from <https://nchica.org/>. Copyright 2017 by Deloitte Development LLC.

Along with the need for medical devices, user acceptance of medical devices is equally important. Feedback is important for software developers to make updates and changes by correlating between healthcare providers, medical device manufacturers, and users to aid in enhancing security in the event of potential technical issues in the software. Hogaboam and Daim (2018) researched user acceptance of medical devices and found that users are mostly positive about wearable medical devices. However, negative feedback on the acceptance of medical devices was due to patients feeling that there was either a lack of or an intrusion in privacy, and often found themselves in the habit of excessively self-monitoring (Piwek, Ellis, Andrews, & Joinson, 2016). Regardless of feedback, medical devices are vital to patient health; and need to securely

share data between healthcare providers and users (Chen et al., 2018). With several types of medical devices used to monitor various kinds of conditions, these devices need a way to communicate and share data amongst other devices.

**Medical devices and IoT.** Advances in sensor technology with medical devices make the creation and calculation of patient data easier for monitoring (Pare, Leaver, & Bourget, 2018). While all healthcare data is important, the collected data is not useful if information cannot be appropriately analyzed. In healthcare organizations, the IoT is a system consisting of internet-connected medical devices used by patients, healthcare providers, and other medical devices to share and exchange data collected through sensors (Razzaq, Gill, Qureshi, & Ullah, 2017). Anything that has the ability to transmit and receive data over a network can be an IoT device, i.e., smartphones, smartwatches, clothes with sensing devices, or electronic pill dispensers. It is estimated that by 2020 there will be more than 25 billion connected medical devices (Khera, 2017). Each medical device has sensors that are used by healthcare providers to track activity, connect to other devices via the internet, process and analyze data, trigger alerts to significant persons, and take appropriate actions if necessary (Farahani et al., 2018; Wang, Kung, & Byrd, 2016). By analyzing and sharing the collected data, the network-connected medical devices become an intelligent system of systems that aid healthcare providers in continuous patient monitoring and accurately diagnosing conditions.

Using medical devices that are interconnected in healthcare changes the way patients and healthcare providers communicate and provide quality of care. However, using medical devices is not without challenges. Khera (2017) discussed how most apps

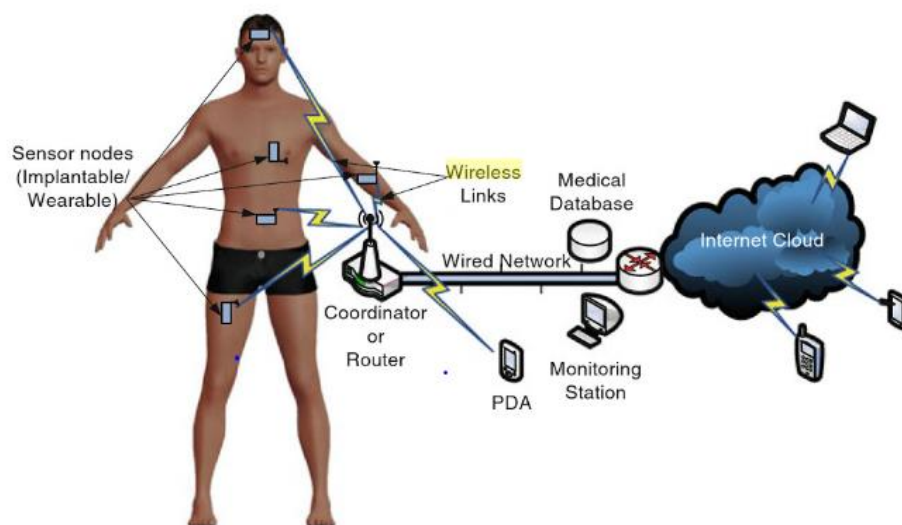
and devices used in IoT are designed with a problem-driven approach rather than using security-driven tactics, which increases the risks of future cyberattacks. Software developers often face technological challenges such as standardization, interoperability, software complexity, wireless communication, and issues with fault tolerance mechanisms when developing medical devices (Kafle, Fukushima, & Harai, 2016; Wan et al., 2016). Tremendous amounts of data are exchanged by numerous medical devices generally over a wireless network. Researchers and software developers continuously work to find ways to keep data and devices secure when data is transmitted wirelessly by medical devices.

**Wireless data transmission.** Whether medical devices are worn externally or internally, some form of communication is required to relay health data to healthcare providers. The data gathered by a medical device is transmitted to other devices and across networks through the use of wireless communication (FDA, 2017). Medical devices using wireless connections can transfer data using cellular/mobile phones, Bluetooth, or Wi-fi in order to support healthcare delivery (Chen, 2017; Anandarajan & Malik, 201). With wireless communication, patients experience the freedom of having instant communication without being in a specific physical location. Health information is conveniently delivered to physicians, patients, or medical staff to monitor critical needs or changes (Grindrod et al., 2017; Lee et al., 2017). Furthermore, wireless data transmission can reach places where wiring would be impossible or too costly, such as rural areas or buildings away from a central location. Panwar, Sharma, and Singh (2016) pointed out that the advantages that wireless data transmission brings to medical devices

are significant for healthcare providers and patients. Still, the main disadvantages are security vulnerabilities and obstruction in the transmission process, which includes physical barriers, climate conditions, or interference. Additionally, Kafle et al. (2016) noted that challenges with medical device data transmission included social factors such as user impacts, privacy issues, and security threats.

The healthcare geography of medical devices is found in hospitals, clinics, homes, remote locations, or mobile. Healthcare providers use wireless technology as a form of communication for cost-effective ways to increase doctor/patient communication from anywhere (Aceto, Persico, & Pescape, 2018; Kumari, Mathew, & Syal, 2017). Medical devices that communicate via wireless connections fall into two categories, either short or long-range. Short-range wireless communication involves data transmission from the medical device or healthcare provider through a local receiver, which is usually near the medical devices (Gomes, Muniz, Silva e Silva, Ríos, & Endler, 2017). Long-range wireless communication involves data transmission directly over the network from the medical device to the healthcare providers' location for monitoring or data storage (Kharel, Reda, & Shin, 2019). Figure 2 shows the flow of how data is collected and

transferred using medical devices.



*Figure 2.* Wireless communication components between medical devices and healthcare providers. Reprinted from *Ultra wideband wireless body area networks* (p. 4), by K. M. S. Thothahewa, J. M. Redoute & M. R. Yuce, 2014, New York, NY: Springer Science & Business. Copyright 2014 by Springer International Publishing.

**Wireless Body Area Networks (WBAN).** WBANs consists of several communication tiers, which means patients using WBANs will have greater physical mobility. The WBAN is composed of external and internal sensors that work together to collaboratively perform patient tracking and monitoring, such as glucose monitoring, blood pressure, pulse, heart rate, and so forth (Aceto et al., 2018). Since the sensors used to monitor various conditions are in close contact with the human body, they are required to use minimum battery power and offer less computing resources (Bhanumathi & Sangeetha, 2017; Sadoudi, Bocquet, Moulin, & Assaad, 2017). The reason for low battery and computing consumption is because merely changing the batteries for implanted sensors requires invasive surgery. With limited computational resources, each

sensor node can process information locally, communicate between nodes, and interact with the environment (Tomovic, Yoshigoe, Maljevic, & Radusinovic., 2017). The sensors worn or implanted is a part of the wireless body area network, which can be thought of as a small network around the patient's body.

The WBAN allows continuous round-the-clock monitoring with real-time updates through approved frequency bands and data rates (Ghamari et al., 2016). The WBAN is used as the gateway communication between sensor nodes (worn on the body) and nearby parent nodes (typically gateways or coordinators) and utilizes short-range or long-range wireless communication for data transmission (Razzaq et al., 2017). The parent nodes transmit data between the small network of sensors and computer applications (Ali, Shah, & Arshad, 2016). Through the WBAN, data is transmitted to healthcare providers with selected routing protocols (Qu, Zheng, Wu, Ji, & Ma, 2019). Routing protocols are essential to increase the reliability between nodes and communication with the healthcare providers in WBANs. Bhanumathi & Sangeetha (2017) surveyed that energy, human posture, network topology, and other characteristics of sensor nodes affect the selection of routing protocols for medical devices. Al-Janabi, Al-Shourbaji, Shojafar, and Shamshirband (2017) advocated that a suitable routing protocol will deliver patient's data without delay or compromising their health. Bhanumathi and Sangeetha (2017) believed that the selected routing protocol security measure should be strong enough to withstand brute-force and reduce computational costs. Effatparvar, Dehghan, and Rahmani (2016) proposed energy-efficient routing mechanisms to prolong the life of a medical device network. Furthermore, Al-Janabi et al. (2017) discussed a two-hop relay mechanism for

a routing protocol that software developers could use to protect the sensor nodes and coordinators from vulnerabilities in the network channel. Routing protocol selection affects the performance and reliability of a medical device wireless network. However, security threats to medical devices can also have a significant impact on the security strategies chosen for medical devices.

### **Risks Involved with Medical Devices**

**Risks using WBAN.** Technical challenges that software developers face in wireless data transmission include keeping the devices reliable, available, and secure while being used to monitor patient health (Dimitrov, 2016; Sametinger et al., 2015). With WBAN being a key player in mobile medical devices for gathering and transmitting data, there are security threats involved that software developers must be aware of to enhance security strategies of medical devices. Threats to data transmitted continue to evolve as technology changes. The threats can be placed in two categories, either passive or active threats.

Passive threats are used by hackers to obtain health information without any modification. For example, eavesdropping is when an attacker intercept and disclose data transmitted (Alaba, Othman, Hashem, & Alotaibi, 2017). Additionally, as a passive threat, a hacker can reroute where transmitted data is sent. Active threats, on the other hand, are attackers attempt to modify data or alter the way the system functions (Kumar, Kaur, Kaur, & Singh, 2016). While eavesdropping, the attacker could tamper with the data sent. Tampering with the messages sent affects the integrity, authenticity, and confidentiality of patient data (Alaba et al., 2017; Rajput & Ghawte, 2017). An attacker



that finds vulnerabilities in the medical device or data transmission process can also generate denial-of-service attacks that affect the availability of critical services. Denial-of-Service attacks can be intentional or due to compromised sensor nodes (Manohar & Baburaj, 2016). A different type of active threat that is harder to catch is insider threats. Usually, with insider threats, a person has legitimate access keys to get inside the system, but may not be authorized (Vithanwattana, Mapp, & George, 2017). An insider threat could alter patient data, withhold information needed to be reported, or cause misdiagnosis or improper treatment. Martin, Martin, Hankin, Darzi, and Kinross (2017) reported that since 2014, the number of cyberattacks in healthcare increased by 300% due to healthcare providers being an easy target. To improve and enhance medical device security, the risks involved with the medical devices need examination.

**Risks using medical devices.** In 2011, there was a major recall of 24 percent of all medical devices due to software failures (Hatzivasilis, Papaefstathiou, & Manifavas, 2016; Klonoff, 2015). A website used to provide software updates for medical devices was compromised. Woods, Coravos, and Corman, (2019) argued that there was a lack of principled engineering practices found in software development that could have lessened the number of medical devices impacted. To keep patient data safe, software developers have to distinguish between safety and security issues in medical devices. Safety involves protecting the medical device user, while security consists of protecting the device environment (Sametinger et al., 2015). The difference is not always clear, especially since security issues can affect the safety of the user.

Security hacks, such as the one demonstrated by security researcher Barnaby Jack, proved how implantable medical devices could be wirelessly hacked and manipulated to cause fatal harm to patients (Burns, Johnson, & Honeyman, 2016). Similarly, security researcher and diabetic Jay Radcliffe demonstrated how security weaknesses found in his own medical device could allow a hacker to deliver fatal doses of insulin to patients (Khera, 2017). In response to numerous vulnerabilities, researchers of the FDA's Office of Science and Engineering Laboratories (OSEL) began developing tools that would aid in spotting security problems in medical device software due to weak designing (Browning & Tuma, 2015). Still, the tools were not enough; the FDA went under heat for not holding medical device manufacturers accountable for poorly secured software (Woods et al., 2015). Williams and Woodward (2015) noted that assuring efficiency and safety while steadily producing new healthcare innovations is problematic to medical device security. Sametinger et al. (2015) pointed out that the use of mobile medical applications is increasing almost at the same rate as the usage of medical devices. The increase in medical applications presents the need for software developers' attention on security measures for the various applications on medical and mobile devices.

**Risks using mobile medical applications.** Mobile medical applications are the software that runs on a web-based or physical mobile platform. The medical application has to meet the guidelines given by the authors of the Federal Food, Drug, and Cosmetic Act (FD&C Act). In the FD&C Act, the authors stated that the application must either qualify as an accessory to the medical device or transforms the medical device platform

(FDA, 2015c). Markley et al. (2017) pointed out that medical application accreditation programs were created to enhance patient and healthcare provider adoption of using medical apps. However, users are still hesitant to utilize medical devices due to perceived security and privacy issues. Vithanwattana et al. (2017) noted that medical device applications that use wireless communication to distribute data are vulnerable to hackers distributing malware. Therefore, researchers have used various techniques to counter and prevent security threats.

Since medical devices can be used virtually anywhere, software developers must analyze preventative measures in the medical application to enhance the security of transmitted data. For example, Li, Wu, Chen, Lee, and Chen (2017) projected that an anonymity authentication protocol used on medical devices would aid in ensuring the security and privacy of user's health data. Similarly, Kang, Jung, Lee, Kim, and Won (2017) believed that an enhanced authentication protocol would strengthen user security and privacy when using medical applications on proxy mobile IPv6 networks. However, further research revealed that flaws found in both authentication protocols could potentially lead to Denial-of-Service attacks (Kang et al., 2017; Li et al., 2017). Based on the various risks that are found between medical devices, the applications running on the devices, and the wireless transmission of data, software developers are in need of advanced security strategies as technology continues to change.

**Additional concerns for software developers.** Medical devices have a significant impact on user's livelihood. However, the security threats and vulnerabilities associated with medical devices are a big concern. According to researchers at the FDA,

it is the responsibility of the medical device manufacturers to identify and address the security risks related to software (Ronquillo & Zuckerman, 2017). Security threats that could affect the confidentiality, integrity, and availability of medical devices could occur at any time. Wangen, Hallstensen, and Snekkenes (2017) discussed the benefit of incorporating risk analysis methodologies to protect, prevent, mitigate, respond, and recover medical data in the event of security threats.

Researchers in many organizations use various methods, such as OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) and CRAMM (CCTA Risk Analysis and Management Method), to assess data security needs. Researchers and software developers, who utilized a risk analysis methodology to evaluate data security needs prior to software development, were conscious of the potential threats and vulnerabilities that could occur (Imoniana & Gartner, 2016; Yang, Ku, & Liu, 2016). OCTAVE and CRAMM are both risk management methodologies that allow researchers to focus on the strategic issues using security practices found in the organization (Singh, Joshi, & Gaud, 2016; Szabo, 2017). Risk analysis incorporates confirming an occurrence, playing out an examination on that risk, containing the threat, remediating the issue, and re-establishing service (Fitzgerald et al., 2017). Wei, Wu, and Chu (2017) explained that finding all possible risks in a medical device is not possible due to human error. However, organizations are challenged with defining the accuracy of their risk analysis plan. Using risk analysis methodologies will help to address vulnerabilities that currently exist in medical devices software.

Due to the sensitive personal information collected, sent, and stored by medical devices, security mechanisms and countermeasures are needed for added security (Li et al., 2017; Sametingler et al., 2015). Mcleod & Dolezel (2018) explained that the most common attack in healthcare institutions are data breaches; in fact, over 100 million healthcare records were stolen in 2015 due to a data breach. Blake, Francis, Johnson, Khan, and McCray (2017) discovered that in 2015, 43% of security breaches on medical devices were due to the devices being lost or stolen. The lost or stolen devices make it easier for hackers to gain a back-door entrance to healthcare databases. One major concern is that medical devices do not possess the appropriate prevention mechanisms to prevent an attack by a hacker. Data breaches are an unexpected and sometimes purposeful release of private information (Bidgoli, 2016). Data breaches can cause reputational damages, potential lawsuits, loss of customers, and violations of medical regulations (Talesh, 2018).

Klonoff (2015) believed that in order to assert data protection, software developers should follow the CIA (confidentiality, integrity, and availability) Triad. Confidentiality provides users with the security that the privacy and the disclosure of sensitive information are for authorized users only (De Filippi, 2016). Integrity ensures that data is not altered by external or internal factors during transmission and reception of data (Moghaddasi, Sajjadi, & Kamkarhaghighi, 2016). Availability is characterized by the degree to which a system or application is operational and usable (Ademe, Tebeje, & Molla, 2016). Talal et al. (2019) emphasized that in addition to the CIA triad, safety and reliability should be added as safety considerations to develop resilient medical device

software. Khan (2017) discussed an architecture-driven approach used to follow the CIA Triad to prevent and reduce confidentiality leaks that could cause significant overhead to keep medical devices secure. While many software developers follow the CIA Triad as a foundation for medical device security, some developers believe that factors for better security are missing. Singh, Kumar, & Hotze (2018) believed that factors, such as vulnerability detection, cost efficiency, security management, and so forth, are difficult to achieve using only the CIA Triad as the foundation for medical device security. Lu, Zhao, Zhao, Li, and Zhang (2015) were against just using the information assurance security attributes proposed by the CIA Triad when applied to medical device security. Khan (2017) justified that for information assurance and security: accountability, trustworthiness, nonrepudiation, and privacy factors should be analyzed along with the elements of the CIA triad.

Healthcare organizations would also benefit from having security mechanisms that could detect security threats in advance. Gopalakrishna-Remani et al. (2018) discussed how technical controls should be the first line of defense to detect security threats in systems. Technical controls are often used as a “set it and forget it” type control and is used to identify device malfunctions in a timely manner. Some researchers believe that technical controls can keep them free from concerns, and often cause software developers to lower their guard against information security risks (Sametinger et al., 2015). As long as the proper focus is not placed on technical control countermeasures, information security will remain a problem (Gopalakrishna-Remani et al., 2018). The controls for technical security risk mitigation can range from simple to

complex measures, engineering disciplines, or security packages that work with the hardware, software, and firmware found in the system (Williams & Woodward, 2015). Technical controls are composed of various methods to detect violations and recover the system, such as automated auditing, intrusion detection, virus detection, system restoration, prevention, and support (Sametinger et al., 2015).

In addition to technical controls, fault tolerance safety measures should be used as the second line of defense in the event that a malfunction surpasses the technical controls in place. Medical devices are made by various manufacturers, using various equipment and software strategies. In the case of using multiple devices that have different software standards, software developers must keep in mind that if legacy systems are not updated to the latest security measures, vulnerabilities can be exposed over the network. The exposed vulnerabilities could lead to attacks on the network and affect other connected devices. Threats or failures on the network or medical device could arise at any moment. Thus, the need for software developers to implement fault tolerance techniques as a fail-safe alternative for medical devices. Fault tolerance techniques involve having a medical device software designed in such a way that the medical device will keep performing fully or at least partially even if one or more parts of the system fail (Diaz, Martín, & Rubio, 2016; Stamate et al., 2018). Fault tolerance can be broken down into two types: reactive fault tolerance and proactive fault tolerance. Reactive fault tolerance reduces the impact of failures by issuing tasks that would aid the system in continuing its job (Kochhar & Hilda, 2017). While proactive fault tolerance predicts potential faults before failures; this is to avoid having to use recovery methods (Kochhar & Hilda, 2017).

### **SST Influences on Security Strategies**

Software developers, federal agencies, and researchers are continuously researching security strategies to lower security risks when collecting, sending, and storing patient information via medical devices. Zhou & Thai (2016) noted that software developers' viewpoints on security adoption directly affected the security of the organizations' information. Many applications and medical devices are designed with security mechanisms to protect patient data (Tewari & Verma, 2016). Researchers have discovered that rapid technological changes in healthcare organizations bring forth challenges and vulnerabilities associated with the privacy and security of sensitive data, as well as how to scale the collection of unprecedented amounts of data from multiple medical devices (Darwish, Hassanien, Elhoseny, Sangaiah, & Muhammad, 2019; Losavio, Chow, Koltay, & James, 2018). In addition to rapid changes, some software developers lack of knowledge or decision against incorporating external factors outside of technological aspects has significant impacts on medical device security vulnerabilities.

When making a decision regarding security strategies, some software developers seek more information on how these devices are used and what influenced decisions made in the past regarding privacy and security measures. Perakslis and Stanley (2016) pointed out that in addition to physical risks, legal liabilities, regulatory liabilities, and recovery costs affects how security measures are utilized for medical devices. Software developers can use methods previously found to overcome the challenges they face when deciding on security strategies to implement in medical device security. Brand (2017)



noted that proactive anticipation and planning in medical device security strategies would assist software developers in limiting cybersecurity defects. Following Brand's concepts on safeguard measures, aspects of the SST theoretical framework that is relevant to this study are also included. The aspects of the SST that are included are the social, institutional, cultural, and economic influences on software developer's decisions regarding medical device security.

**Social influences.** Social influences may have indirect, unintended, or unanticipated effects on medical technology. Not all healthcare organizations are equipped with the necessary tools to handle the risks or changes in technology due to external influences such as end-users, hackers, and current trends. By considering both the risks to medical software and devices and how users and third-party influences have impacted other organizations could assist software developers in the preliminary assessment of social influences with their organization's medical devices.

***Building a team for security.*** Prior to software updates or releases, stakeholders must consider the risks involved with using the medical device and its software. An important consideration is what to do if patient data is hacked, stakeholders can choose to shut the device down, leave the system alone, or update the software. Having a team in place consisting of key experts to figure out how to handle the situation quickly is needed. This team is composed of stakeholders with various experience and specialty areas, i.e., the medical device users, developers, and clinical experts. The purpose of this team is to brainstorm possible scenarios that could interrupt the functionality of medical devices and create an incident response plan to handle these scenarios (Zhou & Thai,

2016; Faiella et al., 2018). Zhou and Thai (2016) referred to a technique called the Failure Mode Effect Analysis (FMEA), used by security teams in various industries, to produce strategies in the event of software failures, attacks, and so forth. These strategies can be incorporated into the security design of medical devices. Software developers in healthcare organizations have a lot of strict guidelines that go into software development and the security of medical devices. Once on the market, plans for security measure updates and maintenance of medical devices need to be addressed for long-term use (Diaconu et al., 2017). So many issues, such as malware attacks, theft of personal information, unauthorized access, and even user tampering, could affect the security of medical devices.

*User influences on medical device security.* When a new technology that could impact the livelihood of many people is introduced, security is a big concern. Research in the field of information systems security examines the use of organizational policies that specify how users of information and technology resources should behave in order to prevent, detect, and respond to security incidents (Cram et al., 2017). Researchers at the FDA stated that vulnerabilities that are undiscovered by developers and users are ticking time bombs that a hacker search for in order to exploit software issues (FDA, 2015c). When software developers are designing the mechanical and software portions of medical devices, they must keep in mind that human factors should be considered in the design. Latif, Othman, Suliman, & Daher (2016) suggested using a user-centered design approach that involves participants in the design process to incorporate changes due to user behavior.

Studies have shown that 78% of Americans are not focused on the security of medical devices (Darwish et al., 2019). User interactions with the medical devices are sometimes in opposition to the developers' and manufacturers' plans for the intended use. Furthermore, user modification could lead to software exploits. Understanding users' interactions with other devices affect user interface designs and the security mechanisms involved. Borsci, Buckle, and Hanna (2016) discussed how some medical device software developers incorporate Human Factors Engineering (HFE) to optimize human influences along with security strategies to enhance medical device performance. Samaras and Samaras (2016) pointed out that the effect of providing medical devices with user interfaces that are effective, efficient, and satisfactory to users often hinders the security of the device. Hatzivasilis et al. (2016) further explained that device misuse by users leads to potential failures of security measures that software developers have in place. Security threats from user influences could destroy the accuracy of information gathered and offset the devices' designed tasks (Klonoff, 2015). User modification to the medical devices to get additional information not intended to be displayed by the device could also lead to other security vulnerabilities.

Handling security challenges is not just a job for software developers, but for all parties involved with its usage, including federal agencies. Researchers at the FDA propose adding security controls to limit access to medical device settings (Williams & Woodward, 2015). Using a layered authorization model based on specific user needs, these security measures would prevent unapproved authorization and implement methods for retention and recovery of device configuration by authenticated users (Chang, Kuo, &

Ramachandran, 2016). While medical devices can be protected from software modification from the users, some mobile devices cannot. Personal mobile devices, such as a patient's smartphone, can be used as the coordinator to bridge the communication between the wireless sensors and the medical database (Chen, 2017). An issue with using personal mobile devices is if the user jailbreaks the device. Jailbreaking is done to remove manufacture and carrier restrictions from the device (Chao, Ho, Leung, & Ng, 2017). In removing certain settings, security layers are removed, and vulnerabilities are introduced to the device (Lee & Soon, 2017). The issue that can occur due to jailbreaking includes malware attacks, theft of personal information, device instability, disruption of services, or unauthorized access to the device (Chao et al., 2017; Lee & Soon, 2017).

*Third-party influences on medical device security.* Third-party influences are individuals, outside of healthcare providers and medical device users, who do not have direct connections with the medical devices. The Health Insurance Portability and Accountability Act (HIPAA) privacy rules are very strict on who can access a system, who can view what records, and who should be making changes on patients' electronic health records (EHR) (Kruse, Smith, Vanderlinden, & Nealand, 2017). Researchers established HIPAA guidelines to set standards of what a person is authorized to access in healthcare organizations, ultimately minimizing insider threats, but what about the outside threats? It is easier than ever for hackers to locate medical devices connected to a network, simply by using the website known similar to Shodan (Genge & Enachescu, 2015). Shodan was a search engine that could be used to monitor network security and to

explore connected devices and corresponding locations (Genge & Enachescu, 2015).

With technology consistently changing, hackers are becoming more innovative in ways to exploit security measures.

Software developers must understand that identification and authentication are just as important as security measures for sharing data with the correct people. The layered authorization model previously mentioned would aid in granting users access to data based on security and role-based authorization methods. On the user-level, software developers should enhance password requirements on medical devices to protect users from dictionary attacks, passwords being guessed, or brute-force attacks (Mahmood, Ning, Ullah, & Yao, 2017). Yang, Lo, Liaw, and Wu (2017) recommended going a step further with two-factor authentication to ensure that only authorized users have access to the medical device even if others know the user password. Additionally, commonly used technical controls such as encryption techniques or usage of VPNs (Virtual Private Networks) adds to the level of security for medical devices against third-party threats. For identification, access controls are recommended by researchers such as Tewari and Verma (2016). Role-based access control grants or limits the necessary capabilities of key people who need access to the users PHI. Role-based access is not strong enough alone, if the wrong person gets unauthorized access to the medical system, that person could steal information, add ransomware to the system, or cause deaths through misuse of medical devices connected to the system (Billingsley & McKee, 2016).

Outside of hackers and the necessary healthcare providers, sometimes users grant third-party access to advertisers at the risk of compromising data. Kane, Bakker, and

Balkenende (2018) pointed out that it is normal for patients to give consent for third-party access to medical devices and applications without understanding the endangerment to data protection. This consent weakens the security measures put in place by software developers. Weininger, Jaffe, and Goldman (2017) believed that the lack of standard application development guidelines is the reason behind security concerns of patient data in medical devices. In addition to social influences, security mechanism choices are influenced by the institutional dynamics, i.e., internal values, strategies, and resources, of the healthcare organization. As stated by Perakslis and Stanley (2016), security and compliance are not the same. Therefore, institutional influences set by researchers covered in the Health Care Information Privacy and Accountability Act are also examined by software developers for security design choices.

**Institutional Influences.** Over the years, medical devices have played a critical role in diagnosing and treating illnesses. Healthcare organizations are engaged in research and development to reach new areas of healthcare. The medical device industry is seen in the therapeutic area, prosthetics, cardiology, drug delivery, and so forth. Most medical devices are regulated by the FDA; however, during the development and launch of medical devices, federal regulations are not always accounted for. It would benefit stakeholders' and software developers' organizations if the regulatory implications and legal liabilities were analyzed sooner rather than later in the medical device development lifecycle.

**Regulatory implications.** Software developers and officials of the FDA are aware of the various security threats to medical devices. They are continuously developing

strategies to limit security threats in order to protect information as well as information systems (FDA, 2015c). Serban (2016) emphasized that there are three challenges associated with medical devices in correlation to federal regulations, which include: (1) compatibility, (2) safety and effectiveness, and (3) the overall cost. Members of the FDA and the Federal Communications Commissions (FCC) have worked together to define policies for medical device manufacturers as a guide on the regulatory requirements for medical device technologies. Researchers at the FDA and FCC released joint statements to discuss how both the wireless and broadband communication methods used in medical devices need to be reliable, safe, and secure (FDA & FCC, 2010). Coburn and Grant (2017) believed that all stakeholders in healthcare organizations, from CEOs to software developers, should understand the regulatory pathways in place before each device is released to the market. These regulatory pathways ensure that the medical devices are consistent with federal regulations and that software developers implement application procedures that facilitate technology advancements while keeping patient security in mind (Coburn & Grant, 2017; He et al., 2019). However, Van Norman (2016) pointed out how researchers at the Institute of Medicine believe that the pre-market approval given by the FDA does not assure device safety.

To know what has been done and what may be needed in the future, federal agencies are requiring medical device manufacturers to provide risk analysis for each device (Sametinger et al., 2015). By knowing the risks associated with the devices, this sets in place a plan on how to address unidentified and identified risks to these medical devices. To enforce the creation of the risk analysis report, not providing documentation

could delay the device from going to market. Researchers at the National Institute of Standards and Technology, also known as NIST, worked directly with medical device stakeholders to set standards, procedures, and policies to reduce cyber risks when using medical devices (Kohnke, Sigler, & Shoemaker, 2016). Under 47 CFR part 2, medical devices using radio frequency (RF) communication must operate in compliance with the Commission policies and operate without causing harmful interference (The Departments and Agencies of the Federal Government, 2017; FCC, n.d.). Equipment authorization using RF communication includes several steps, such as understanding FCC rules to determine if the rules apply to the medical devices, perform necessary tests for compliance and approval, labeling and understanding manufacturing/importation requirements, and modifying as needed for additional approval (FCC, n.d.).

Like technology, the medical field is ever-changing, which means that existing technology must be modified to meet the security needs of these changes. Identification and authentication used in a security framework are not typically discussed and covered in an over-the-network setup (Misra, Goswami, Taneja, & Mukherjee, 2016). However, identity management is needed to safeguard information and to provide the necessary tools needed for individual setup (Rong et al., 2013). In the medical field, software developers must ensure that they are following HIPAA (Health Insurance Portability and Accountability Act) guidelines (Moore & Frye, 2019). HIPAA has strict guidelines on who has access to a system, what they can view, and hold healthcare staff accountable (Moore & Frye, 2019). If a nurse was to access a patient (they may or may not know



personally) that is a direct violation of HIPAA laws, this could lead to termination and possibly a lawsuit against the organization (Moore & Frye, 2019).

***Legal liabilities.*** Developers of private health apps will generally not be subjected to medical malpractice claims since malpractice concerns the physician-patient relationship (Terry & Wiley, 2016). However, developers could face their own types of liabilities. According to the researchers at the FDA, medical device manufacturers are responsible for identifying and addressing security risks associated with the software (Ronquillo & Zuckerman, 2017). In addition to potential liabilities for violating the FDA's medical device regulations, developers of medical device applications are likely subjected to available product liability claims, including design defects, breach of warranty, and failure to warn (Terry & Wiley, 2016). Legal liabilities limit the expansion of medical device applications, as well as shift focus on ways to minimize risks for developers (Bertolini et al., 2016; Terry & Wiley, 2016; AlTawy & Youssef, 2016). AlTawy and Youssef (2016) explained that if legal issues are a threat to medical device expansion, researchers at the FDA will issue either a warning letter or recall from developers whose software does not comply with regulations.

Healthcare information is commonly stolen to gain personally identifiable information (PII). Hospitals and healthcare organizations are notorious for putting cybersecurity in the background in order to prioritize operations in the facility (Williams & Woodward, 2015). Researchers at the FDA release policies and standards which define the roles, responsibilities, and activities needed to address data and system security measures on a network where medical devices are used (Bolon et al., 2018).

Additionally, researchers at the FDA recommend that developers of medical devices in healthcare organizations should check the FCC website when developing software for new specifications and updated information (FDA, 2017). Federal regulations and cultural influences work together to influence how medical device creation and security is handled in the United States. The cultural influences on medical device security vary between different organizations.

**Cultural influences.** Cultural influences in healthcare organizations are composed of shared beliefs among the employees, and those beliefs are supported by strong strategies and culture. Most organizations have strong core values that start with upper management and stem down to new employees, starting with the recruiting and selection of potential employees. Cultural influences in an organization affect how situations are responded to and the expected behavior which aligns with the core value. Strategies for selecting medical device security is indirectly influenced by organizational culture and directly influenced by organizational strategies

**Organizational culture.** Employees of every healthcare organization build their own culture over time. The culture reflects the core values of the organization based on factors such as beliefs, assumptions, perceptions, thoughts, and feelings (Matko & Takacs, 2017). Software developers follow the guiding principles of the organization and adapt to the way things are done in that organization (Hignett et al., 2016). The established culture of how tasks are handled in a medical device organization affects the way decisions are made. For example, some stakeholders may be more focused on customers' perceptions of the medical device over regulatory compliance.

Organizational culture is learned, and it continues to evolve as software developers gain experience. Rothrock, Kaplan, & Van Der Oord (2018) believe that consistent training for the organization, developing a common language for security expertise, and understanding security versus resilience mechanisms for medical devices shape the cultural influences of an organization. According to Karlsson, Kolkowska, and Prekert (2016), medical device software developers have to view data security from two different viewpoints: (1) the point of the individual user level of information security and (2) the level of information security approaches. Security threats can occur from a lack of knowledge of security standards. Researchers, such as Kartolo and Kwantes (2019), believed that various company initiatives, such as security units, security commitments, organization-wide security processes, and security awareness programs, shape and mold the organizational culture and enhance security strategy selection. To succeed in medical device security, stakeholders in the organizations must be able to adapt to changes rapidly (Auer & Jarmai, 2015).

***Organizational strategies.*** Due to security attacks, an organization could be faced with lawsuits because of (a) data breaches, (b) profit loss, (c) recovery cost, and (d) fines imposed by federal agencies (Zeadally, Isaac, & Baig, 2016; Chang et al., 2016). To anticipate security breaches, stakeholders need to understand the importance and cost associated with ensuring up-to-date preventative measures. Not only that, but developers must understand the influences of design choices and organizational decisions when implementing a system. Bergh et al. (2016) suggested the use of empirical research which identifies problems or questions through observation, studies significant decision

points, derive conclusions based on research, performs tests using several decision points, and evaluate the outcome.

Kakucha and Buya (2018) identified deterrence, prevention, surveillance, detection, response, deception, perimeter defense, compartmentalization, and layering as strategies software developers should use to enhance security strategies. These strategies are adapted and utilized based on learned behavior within the organization. Learning from past mistakes, current trends, social impacts, and possible threats could influence the way the security of the system is enforced. Deterrence and prevention both aim to protect and prohibit attacks while using disciplinary actions as influences (Maheshwari, 2016). Surveillance and detection identify security vulnerabilities through systematic monitoring and allows fast responses to threats (Sametinger et al., 2015; Sung, Sharma, Lopez, & Park, 2016). Response and deception take corrective actions while distracting the attacker's attention away from critical information (Kakucha & Buya, 2018; Sherman et al., 2017). Perimeter defense, compartmentalization, and layering all assist with regulating the network traffic, reducing hacker's opportunities to attack, and using multiple countermeasures that work independently to increase effective defense against attacks (Roman, Lopez, & Mambo, 2018).

***External culture.*** For security design, software developers have to take into account the cultural diversity of users as well. Issues between the intended design and actual usage of medical devices by medical device manufacturers, as well as the regulations imposed by federal agencies, cause problems for software developers (Williams & Woodward, 2015). Stakeholders' goals are to provide the innovation that

users and healthcare providers want for the devices, while also ensuring efficiency and safety; however, this task proves to be challenging. Clinical trials are not needed for medical device approvals; however, in the U.S., medical devices are required to pass pre-market submissions and post-market surveillance (Seltzer et al., 2017). Before medical devices are placed on the market, each device must meet standards given by researchers at federal agencies such as the FCC and the FDA.

To keep up with customers' needs, software developers at a manufacturing company had the idea to create a modular architect for their medical device that could be configured to the consumer's need at that moment (Robinson, 2015). Consumer's started off with basic devices unless enhanced features were needed/wanted. If requirements changed or more functionality was necessary for the medical device, the consumer could come back and get the device upgraded (Robinson, 2015). The modular approach also handled security updates needed as technology progressed. The concept was to save the consumer money initially and bring in more money with upgrades. However, this did not happen. Most customers chose basic needs and opted out of the upgrades due to the current trends, causing the manufacturer to lose a lot of money (Robinson, 2015). In this case, the manufacturers saw the potential monetary benefits if the modular approach was useful for the users to add on features over time. Researchers such as Latif et al. (2016) believed that software developers should look at external factors such as healthcare providers' behavior, how security policies affect the healthcare given, and how users are affected by certain security measures before. Along with cultural influences, the

strategies involved with the development of medical device software are affected by economic influences.

**Economic Influences.** Economic influences on business decisions occur whenever that decision is affected by any economic factors, such as constraints and budgets. Software developers' decisions on security strategies for medical devices are influenced by a wide variety of causes; however, cost is always a major factor. Technology impacts economics just as much as economics impacts technology. The primary goal of most medical device organizations is to design, produce, and ship devices as soon as possible to see a return in revenue. To get medical devices on the market, medical device manufacturers have to overcome barriers such as regulatory standards, new and complex changes to technology, and quality in order to sell their products at a reasonable price to compensate the efforts (Diaconu et al., 2017). Van Norman (2016) noted that some medical devices costs between \$10 and \$20 million for development and testing. Software developers and stakeholders face pressures for cost containment when selecting security mechanisms for medical devices (Johnson, Belin, Dorandeu, & Guille, 2017a). Patients often believe that healthcare providers are suggesting medical devices that are safe but are not always open to price changes for medical devices or services due to enhanced security (Johnson et al., 2017a). The choices for medical device security mechanisms are decided by many factors including costs; however, potential future costs must also be considered. A single data breach can cost healthcare providers millions per incident. Osborn and Simpson (2018) reported that despite knowing the associate economical risks, some stakeholders in medical device organizations only have intentions

of increasing security budgets in the event of a security breach or threat, not in the initial stages of planning and development.

Medical device providers work to keep the systems they support accessible and reliable at all times by minimizing hardware failures and having strategies to lessen software issues (Talesh, 2018). Sametinger et al. (2015) argued that medical device data would never be 100% secure due to unknown vulnerabilities in the software and transmission process. Data encryption was mentioned as a proposed solution to vulnerabilities in the software and transmission process. However, encryption technology is often avoided due to the cost of hardware and software needed to support it (Raza, Kulkarni, & Sooriyabandara, 2017). It was found that medical device manufacturers and software developers spend a considerable portion of time and money to enhance security procedures later rather than sooner (Singh, Kumar, & Hotze, 2018). When problems such as device malfunctions occur, the device can be protected and fixed quickly, but security exploits and vulnerabilities are not always easy to detect (Bidgoli, 2016). Malware can be placed on the system in a dormant state and can cause harm at unexpected times. Creators of the Health Information Technology for Economic and Clinical Health (HITECH) Act imposed regulatory penalties in efforts to increase security efforts during the development process of medical software. Lin, Lin, and Chen (2019) noted that the penalties set by HITECH have had limited effects due to only a few extensive regulatory actions that have been taken against medical device organizations.

Social, institutional, and cultural related decisions are also affected by economic influences. Some medical device manufacturers will spend millions just to meet the

criteria imposed by federal agencies. Security updates to keep up with user needs and federal regulations can be costly due to how changes are distributed. Users tend to keep older devices as long as they are functioning as required to avoid costs. Despite the new development and increased usage of medical devices, medical device manufacturers continue to attempt to make the devices more cost-effective for users (Sametinger et al., 2015). Nevertheless, increasing interconnectivity between medical devices cost manufacturers more money to maintain security between new and legacy systems. Providing support to the cultural influences via training and development activities is costly in time and money, and can decrease overall security quality (Sametinger et al., 2015). Taking the quick path to getting the medical devices on the market can be costly due to security vulnerabilities that are sometimes missed. McLeod and Dolezel (2018) stated how a hospital in New York was fined over 4 million dollars due to patient data breaches and poor risk analysis performed on hardware and software. Software developers need to know in advance the economic implication their security design choices could add to the development process. Though, the final decision on security measures is not always up to the software developers. Healthcare providers could decide against specific security measures due to costs or not seeing the economic value in particular design choices. Some healthcare providers admit that there is a limited budget for healthcare data security (Osborn & Simpson, 2018).

### **Transition and Summary**

This section included the background, purpose, and intended approach for this study regarding strategies software developers use to implement security measures on



medical devices. Medical devices offer many benefits to healthcare providers and patients; however, the security of the data collected and transmitted by these devices raises major concerns. Security strategies were examined in this section to understand mechanisms typically used for medical device security. Additionally, a review of the SST was conducted, which included the changes, opposition, and usage of the theory. Finally, the four factors of the SST theory were used to analyze how external factors may influence the direction of innovation, the practices used by software developers, and the outcomes of technological decisions.

Section 2 will include information on the study's purpose, the role of the researcher, participants selected for the study, research design choice, and data analysis methods used to study medical device security strategies. Section 3 will include an overview of the study, the findings of the research, and how it not only applies to professional practice but can potentially improve information technology practice. Additionally, section 3 will include the implication this study has for social change, recommendations for future research, and my reflections of the study.

## Section 2: The Project

Section 2 adds on to Section 1 by defining specific techniques and methods used in the study to ensure quality research. In section 2, I define information on the researcher's role in the study, how participants were selected, and what research and data analysis choices were chosen. In addition, I examine information on the research methods, research design, and how data was collected and organized to present the findings. Finally, I review strategies to assure the reliability and validity of the study.

### **Purpose Statement**

The purpose of this qualitative exploratory multiple case study was to explore strategies software developers use to implement security measures to protect patient information collected, sent, and stored by medical devices. The population for this study included software developers whose primary focus was on the security aspect of medical device software in three software companies in the Baton Rouge, LA, area. The software developers participated in open-ended interviews to discuss their strategies for and viewpoints on securing the software in medical devices. Company documents were also reviewed to gather additional information on security strategies to triangulate the data. The implications for positive social change are that new strategies may limit the exposure of private PHI from unauthorized users.

### **Role of the Researcher**

The researcher in a qualitative study is considered an instrument used in the data collection process (Lewis, 2015). As an instrument, data is intercepted by the researcher rather than questionnaires, computer systems, and so forth. (Lewis, 2015). In this study, I

was the instrument used to collect data by conducting a case study. Sanjari, Bahramnezhad, Fomani, Shoghi, and Cheraghi (2014) noted that there is not a single way of conducting qualitative research; in fact, the way qualitative research is carried out depends on factors that affect the researcher, such as beliefs, knowledge, purpose, goals, and audience. My responsibility included designing the study, developing interview questions that answered the overarching research question, selecting participants, examining feedback, and eliminating researcher bias. In removing any personal bias from the study, I ensured that the findings were presented from the participant's point-of-view.

I have 6 years of professional experience in the software industry in various industries such as Oil & Gas, Federal, and eCommerce. Prior to this study, I did not have any software development experience in the healthcare field or with medical device software development. A researcher who has experience with their topic can negatively affect the study, mainly because their experience can influence the outcome of their study (Chenail, 2009). Due to not having any experience with medical device software and minimal experience with security strategy selection limited any researcher bias I might have brought to this study. Initially, my interest was in robotic software security to help those with disabilities live normal lives due to having an uncle who was confined to a wheelchair. I shifted towards medical devices after learning about various medical devices that work together or independently and the occurrences of security hacks on these devices.

I established that all conducted research and data collection was performed ethically. I followed the guidelines in the Belmont Report in order to establish that the research and data collected for this study were gathered ethically (National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, 1979). The Belmont Report consists of guidelines for handling research that involves human participants. Sanjari et al. (2014) discussed various ethical challenges that are found in all stages of a qualitative study, which included confidentiality, anonymity, informed consent, the potential impact on participants and organizations, and so forth. I ensured that participants and the organization remained anonymous in the study. Furthermore, I guaranteed that I was following the three ethical principles of the Belmont Report, which includes (a) respecting the participants of the study and assuring informed consent to the study, (b) beneficence by insisting participants are treated ethically, and (c) justice for participant selection. To ensure ethical considerations regarding human participants as codified in the Belmont Report, many institutions and organizations developed an IRB (Lincoln & Tierney, 2004). Getting approval from Walden's IRB before beginning my study certified that ethical considerations regarding this study were met. Additionally, I completed the training course Protecting Human Research Participants (certification number: 2073402) given by the National Institutes of Health (see Appendix A).

In qualitative research, the study can be at risk of bias from the researcher based on how information is interpreted. According to Podsakoff, Mackenzie, & Podsakoff (2012), researcher bias is a form of response bias that can occur when a researcher has familiarity with the research topic being studied. Researcher bias was limited in this

study because while I have a background in software security, I have limited experience in security strategies for medical devices. This factor alone reduced bias and aided in the research process. While the company I worked at the time of this study had departments consisting of software developers that work directly with security strategies, I completed this study using organizations with which I had no associations. When a researcher has connections or works for the company being studied, confirmation bias could occur. Confirmation bias occurs when a researcher acknowledges participants' responses that confirm their belief in a study (Denscombe, 2014).

For my doctoral study, my goal was to understand and present all findings from the participants' point-of-view. I selected participants who were accessible, had information that could inform this study, and were willing to share relevant information. To further reduce researcher bias, I reviewed the interview questions to confirm that they would be useful for capturing the entire scope of the research topic without asking any questions that could possibly guide the respondents' answers (see Podsakoff et al., 2012). I conducted open-ended interviews, as mentioned by Thomas (2017), to allow participants to contribute detail information on the study. The open-ended interview style allows the researcher to ask probing questions as a follow-up to participants' responses (Tran, Porcher, Falissard, & Ravaud, 2016). Also, as a researcher, I was cautious not to misinterpret the collected data based on my own feelings towards the subject. After reevaluating participants' responses, I ensured that the conclusions made were from the collected data and not from my experience.

## **Participants**

In qualitative research, participant selection is based on who can best inform the research questions and enhance understanding of the phenomenon under study. Decisions on participant selection are based on what research questions and theoretical perspectives are deemed necessary to complete the study and also how the participant's experience will inform the study (Palinkas et al., 2015). Along with participant selection, it is important to select an adequate sample size to fully inform the study (Malterud, Siersma, & Guassora, 2016). This study included interviews with medical device software developers who focused on or had experience with the security aspect of medical software in three software companies in the Baton Rouge, LA, area. The participants selected to be interviewed had a minimum of 2 years of experience in software security. Choosing participants with various levels of expertise expand contributions to a study (Malterud et al., 2016). I used demographic questions to establish the participants' background and to confirm that the participants were knowledgeable of the subject and could provide valuable feedback (Robideaux, Robin, & Reidenbach, 2015; Yazan, 2015).

The POC is the person who acts as a representative of the organization that can be contacted via phone or e-mail when an event occurs or needs arises (Denscombe, 2014). According to Denscombe (2014), the POC should be a person in the organization who could be approached for assistance with finding participants and other information that would be beneficial to the study. Connecting with a potential POC in each organization occurred after receiving approval from Walden University's IRB (approval number 12-

06-18-0548609). After securing the POCs, I received names of potential participants based on the criteria needed for my study (i.e., various levels of expertise, years of experience, decision responsibility towards security strategies, and so forth). To create a working relationship with participants, I worked with the POC of the organization for initial contact. I provided the POC with an e-mail invitation to be forwarded to potential participants along with a consent form for each eligible participant to sign. After receiving an e-mail response from participants on their participation, I worked with each participant to arrange a time for each interview. Also, I offered a time to meet prior to the interview if the participants had any questions. If participants replied to the e-mail without signing the consent form, I sent a secondary e-mail, which included the consent form and guidelines for the study.

The purpose of the consent form was to confirm that participants involved in the study met the criteria set by the IRB. The IRB is responsible for assessing research studies that involve people and verifying the study complies with both federal regulations and ethical principles (Nebeker et al., 2016). As the researcher and interviewer, it was important to ensure participants were comfortable and understood the purpose of the interview. To create a comfortable environment, I began by explaining the importance and procedure for keeping their information and responses private in the study. Giving participants a sense of protection by knowing their information will be confidential and anonymous, builds the participants' trust in the researcher (McDermid, Peters, Jackson, & Daly, 2014). I reminded the participants that the interview would be completely voluntary, and their identity and organization would remain confidential in the study.

Each time I spoke with or e-mailed the participants, I was sure to offer the participants the chance to ask questions. Also, I made sure to summarize the interview process at the time of scheduling the interview, as well as before the interview began. Building rapport between the researcher and the participants creates a mutual trust, which can make the participant comfortable enough to provide lengthy, informative information to the researcher (McDermid et al., 2014). The main way for me to develop a working relationship with each participant was by making sure that the participants felt comfortable. Making sure that the participants were comfortable made the participants provide more in-depth information related to the research study.

### **Population and Sampling**

The population of my study consisted of software developers who focused on or had experience with the security aspect of medical device software. Selecting applicable participants to a study aids in maximizing the depth and richness of information gathered for a study (DiCicco-Bloom & Crabtree, 2006). Specifically, this research study targeted software developers from multiple organizations, all working with medical devices. Sociologists have made claims that not all participants are able to observe, understand, and interpret experiences in a way needed for a study; therefore, participant selection is essential (Saunders, 2012). Participants were selected for this study based on who could best inform the research question. The selection process of participants must reflect the purpose of the study in order to find the appropriate individuals that would aid in the research topic investigation (DiCicco-Bloom & Crabtree, 2006). The population in this



study included software developers who have knowledge of security strategies to lower security risks involving medical devices used for patient care.

Nebeker et al. (2016) emphasized that a researcher must identify and specify the characteristics participants must possess to be considered partakers in the study. Having ineligible participants may negatively impact the reliability and validity of data collected in the study. Thomas (2017) discussed the importance of having participants that are openly willing to share information. To attest that I had qualified participants in my study, I utilized a selection criterion to distinguish eligible participants. Several eligibility criteria had to be met for participants to participate in this study, which included (a) working at the organization chosen for this study, (b) working with medical device security, (c) having knowledge on security strategies used to secure data collected, sent, and stored on medical devices, and (d) willing to share their experiences with medical device software security. Additionally, the population for my study had to have a minimum of two years of experience in software security to provide insight into the research.

A criterion-based sampling strategy was used to certify that the participants in this study met the criteria to be eligible to participate in this study. Criterion-based sampling adds benefits to a qualitative study by guaranteeing that participants selected meet the pre-selected assessment for participation in the study (Cleary, Horsfall, & Hayter, 2014). The population of this study consisted of software developers from three organizations in Baton Rouge. I selected three to four participants from each organization to participate in interviews for this study. All of the participants chosen for this study met the criteria for

participation eligibility. The driving principle for choosing an adequate sample size for qualitative research is the total participants needed to reach data saturation (Thomas, 2017). In a qualitative study, a large number of participants can be irrelevant to the study because more participants do not always lead to the occurrence of more data (Morse, 2015). The sample population for this multiple case study consisted of 10 software developers from the Baton Rouge, LA, area. Different participants can have diverse opinions about a phenomenon that can uncover valuable information relevant to the study (Thomas, 2017). However, with a large sample size, data collected can become repetitive and unnecessary (Galvin, 2015). To reach data saturation for the study, I interviewed participants until no new information was presented on the topic.

I made the interview process as comfortable as possible for the participants. Hesitation from participants can negatively impact data collected. It is best to establish rapport with the participants before the interview begins (Saunders, 2012). Taking the time to gain trust allows the participants to feel comfortable enough to openly share information with the researcher (Thomas, 2017). I introduced myself to the participants in my study and was opened to any questions they may have had about me as the researcher or about the study. External factors, such as location or distractions, can have a negative effect on the outcome of the study. The researcher should try to find a “safe zone” location, which is free from distractions and makes the participant comfortable to open through the interview (Pitts & Miller-Day, 2007). Hence, I made all attempts to interview participants in a comfortable location where there were no distractions in order to collect information without disturbances. I found that instead of having a set location

and time, participants had more availability if the interview was conducted over the phone.

For this study, I collected data from multiple sources, i.e., interviews and company documents. Collecting the data from various sources aide; in the triangulation and saturation of data. Data saturation can occur when data triangulation includes enough data from multiple methods of data collection to not emerge any new data (Carter, Bryant-Lukosius, DiCenso, Blythe, & Neville, 2014). In semi-structured interviews, pre-determined questions are asked; however, the researcher can go off tangent to ask additional questions that may enhance the study (Massis & Kotlar, 2014). DiCicco-Bloom and Crabtree (2006) indicated that due to the open-ended interview questions used in a semi-structured interview, the interview could take anywhere from 30 minutes to several hours to complete. My interviews took anywhere from 20 to 40 minutes to complete. Additionally, company documents revealed valuable information to the study, which included past security issues, strategies used to protect security vulnerabilities, and how decisions were made. Individual in-depth interviews were used in this study to reconstruct participants' perceptions and experiences of the phenomenon. The overarching research question can serve as the initial interview question to get the conversation going; however, 5 to 10 more questions are needed to indulge deeply into the research issue (DiCicco-Bloom & Crabtree, 2006). Since qualitative research collects data using an iterative approach, a researcher will know data saturation has been met when no new information is gathered from participants (Tran et al., 2016). I used an

iterative nature to conduct this qualitative study to affirm I reached data saturation of the research topic.

### **Ethical Research**

Ethical research was conducted to protect the participants in the study. As a part of Walden University's research ethics and compliance policies, the IRB ensures research ethics of standards are met in the study. First, Walden University requires all students performing research to complete the training course Protecting Human Research Participants. Next, IRB approval has to be granted for the study to ensure that the research topic is deemed ethical. After that, research cannot begin until the letters of cooperation are signed by a representative of each organization and sent back to the IRB board for approval to contact participants. Finally, after IRB approval of the letters of cooperation, consent forms have to be signed by each participant.

I completed the Protecting Human Research Participants course (certification number: 2073402) given by the National Institutes of Health (see Appendix A). The IRB's primary focus is to protect human subjects that participate in research studies from any type of harm (Zhang, Huett, & Gratch, 2018). I obtained IRB approval from Walden prior to collecting any data from participants of the organizations selected for this study. After IRB approval of the letters of cooperation signed by representatives of each participating organization, a consent form was sent to each participant and required to be signed before the study began. IRB consent is necessary for a research study to verify that ethical standards are upheld when human subjects are involved in research (Blackwood et al., 2015). Research cannot begin without the participant reading and

signing the consent form acknowledging their understanding and right to withdraw at any time (Nebeker et al., 2016). The consent form contains information on the intent of the study, confidentiality measures, the participants right to withdraw, along with the benefits and risks associated with this study (Blackwood et al., 2015). The consent form was sent through email, which each participant had to reply with “I consent” in the email in order to participate in the study. Signing "I consent" acknowledged participants' understanding of the scope, expectations, and rights for the interview process. If any of the participants would have withdrawn from the study, any information collected from or about the participant would have immediately been destroyed. Mathauer and Imhoff (2006) stated that incentives often exploit interviewees for personal gain. Informing participants that information gathered will add to the contributions of the research instead of offering incentives increased the accuracy of the information given (Mathauer & Imhoff, 2006). No incentives were given to participants in this study to avoid coercion or fabrication of collected data.

Any information that would reveal the identity of participants or organizations in the study were removed in order to protect the confidentiality and privacy of participants in the study. Researchers need to guarantee a participant’s anonymity in the study in order to keep that person untraceable to any data presented in the study (Saunders, Kitinger, & Kitinger, 2015). Instead of using real names, code names were given to participants (i.e., O1\_P1, L\_P1). The actual names of the participants and the associated code names were stored in an encrypted spreadsheet, which I am the only person with access to the spreadsheet. Assigning organization numbers and participant numbers as

code names assured confidentiality and privacy of both the organization and participants. Lancaster (2017) stressed that the anonymity of the interviewee is critical and must be maintained because the interviewee could possibly share information that could jeopardize their job or the organization they work for. Information collected from participants and company documents will be stored on a password-protected flash drive for five years after CAO approval. This timeframe is used as another step to protect the participants' and organizations' confidentiality in the study. Additionally, the flash drive and physical data collected will be stored in a lock storage cabinet. After five years, all physical and electronic data, including signed consent forms, information collected from interviews, and company documents, will be destroyed.

## **Data Collection**

### **Instruments**

For the purpose of data collection, I was the primary instrument for this qualitative research study. Zohrabi (2013) noted that in some qualitative research, the researchers are the data collection instrument. As the research instrument, researchers must develop, maintain, and eventually close the relationships with the participants (Pitts & Miller-Day, 2007). Data collection came from two places, through semistructured interviews and the analysis of company documents. During the semistructured interviews, I asked open-ended questions to understand the research topic from the participant's viewpoints. Semistructured interviews include the use of open-ended questions so the researcher can gain an understanding of the participant's experiences and encourage broader feedback (Nebeker et al., 2016). Researchers' goals after collecting

data are to extract and categorize vital information to introduce themes from the data (Zohrabi, 2013). As the primary data collection instrument, I collected, organized, and analyzed the data collected in this study to answer the research question.

I created an interview protocol (see Appendix B) for this study that served as a guide of what to do prior, during, and after the interview process. The interview protocol contains a list of interview questions that must be asked during the interview (Castillo-Montoya, 2016). Due to the semistructured nature of the interview, I had the flexibility to add probing questions that would gain further insight into the research topic. Huddy et al. (2015) believed that an interview protocol should be refined to fine-tune interviews. Interview questions in the interview protocol should align with the research question and should be organized in a way to create an inquiry-based conversation dynamic between the researcher and the participant (Castillo-Montoya, 2016). Prior to the interview, a self-introduction, verification of signed consent, an overview of the study, and what was expected was discussed.

The interview began, and I started recording with the participant's consent. The participants were identified on the recording by code names only. Additional questions were added to the interview based on the participant responses. After the interview was complete, the participant was informed of the next step in the study, which included an analysis of the collected data, then member checking. Prior to data analysis, transcription of the recorded interviews occurred. I made sure to take notes of anything that I might have needed to be clarified or expanded on and presented those notes to the participant during the member checking interview. Member checking was used to endorse that

researcher bias was limited and that my analysis detailed that participant perception. Member checking is used to explore the credibility and accuracy of results and ensures that the results resonance with the participant's experience (Birt, Scott, Cavers, Campbell, & Walter, 2016). Simpson and Quigley (2016) described member checking as a back and forth conversation between the researcher and participant to validate the accuracy and interpretation of data gathered. Member checking interviews were repeatedly scheduled until the participants confirmed that my analysis of the audio recordings reflects their experiences accurately.

The audio recording of each interview was saved as a personal reference throughout the study. Recorded interviews allow the researcher to continuously revisit the interview for the purpose of data checking and to consistently portray participants' accounts of the phenomenon (Noble & Smith, 2015). Audio recordings are used to achieve accuracy when analyzing and presenting the findings from data collected in the interviews (Ranney et al., 2015). I used a phone recording app during the interviews in order to focus strictly on the interview and to corroborate the accuracy of my findings. Audio recordings can always be used to match transcriptions to verify accuracy in the data analysis phase of research (Simpson & Quigley, 2016). These recordings aided to verify that I accurately transcribed the interview data.

In this study, the primary data collection method was through the use of semistructured interviews. The primary source for qualitative data can serve the purpose of conveying participants' perspectives on a phenomenon. Still, the primary source should not be looked at as the only method for producing qualitative data (Polkinghorne,



2005). The study included semistructured interviews to collect data and gain insight into the perspectives of software developers who use strategies for medical device security implementation. The semistructured interview method is one of the most popular choices of qualitative researchers for data collection due to the structure of the interview being both versatile and flexible (Kallio, Pietila, Johnson, & Kangasniemi, 2016). For a semistructured interview, there should be pre-requisite questions that will be used in the interview to answer the research question (Castillo-Montoya, 2016). However, the researcher should use opportunities to ask follow-up questions (Castillo-Montoya, 2016). I asked the participants follow-up questions when necessary for clarity of previous responses, and I was careful not to interrupt participant responses. Due to the flexible nature of semistructured interviews, I refined the interview protocol as needed during the interview to certify that questions were clear, and the answers covered the research topic.

A secondary collection method came from the reviewal of company documents. Adding a secondary source for data collection aids in the validity of themes extracted from the collected data during the final analytic work of the researcher in a qualitative study (Yazan, 2015). I established the reliability and accuracy of the data collected in the interviews by performing member checking. The secondary data from the company documents were used to verify findings in the interviews. The triangulation of multiple data sources in qualitative research demonstrates a comprehensive understanding of the research topic (Carter et al., 2014). Triangulation of the primary and secondary data sources occurred in this study to reach a comprehensive understanding of the research question.

Reliability in an interview is established when the same results are obtained with the same respondents if the interview was given again; whereas, validity assures that the instrument in the study gathers adequate data to inform the research (Dikko, 2016).

Reliability was established through member-checking, and validity was provided through the triangulation of data collected from interviews and company documents. The review of company documents was used to support data collected from interviews and aid in explaining the security strategies used by software developers in medical device security. I used these documents to inform my study by uncovering influences that caused specific selected security strategies to be used in the past. Document analysis in qualitative research require the data to be examined in a way to elicit meaning and develop empirical knowledge to explain a phenomenon (Wohlin & Aurum, 2015).

### **Data Collection Technique**

Along with the use of open-ended interviews, data was collected by reviewing company documents and archival records. According to Kamalodeen and Jameson-Charles (2016), a researcher typically conducts a qualitative study in order to gather information beyond simple descriptions. One way to collect data and uncover additional information is through the use of interviews. An interview is used to collect information based on the interpretation of the interviewee, which has proven to give further insight into a phenomenon (Castillo-Montoya, 2016). The objective of this study was not to just find the solutions for the defined research topic but to find other rational explanations of the issue. Building rapport with participants involves mutually gaining trust and respect for both the participants and the information shared (McDermid et al., 2014). Interviews

should begin with basic background questions about the participant; the goal is for the researcher to build rapport with the participant while collecting background data (Castillo-Montoya, 2016). It is important for the researcher's demeanor to remain neutral during the interview in order to not dissuade the participant from their initial response (Doody & Noonan, 2013). In a semi-structured interview, researchers are able to adjust interview questions based on participants' responses (Kallio et al., 2016). I actively listened to the participant's responses and made adjustments to the interview protocol if probing questions could be asked to gather more information on the research topic. After asking additional questions, I returned to the interview protocol and continued asking the pre-determined questions until I reach the end of the list.

I ended the interview with an open-ended question to see if the participants wanted to share additional information on the topics covered in the interview. I asked the participant if there were any company documents that could be shared that would be relevant to the research topic. Next, I explained the concept of member checking to the participant. Member checking is a form of quality control used in qualitative research. With member checking, the participant has a chance to review the information given in the interview and can make changes to improve the accuracy, credibility, and validity of their answers during the interview process (Zohrabi, 2013). The researcher summarizes answers given by the participants, and the participants confirm that the summary reflects their views and experiences (Houghton, Casey, Shaw, & Murphy, 2013). After explaining member checking to the participant, I turned off the recorder and thanked the participant for being a part of this study.

Prior to analysis, recorded data needed to be transformed into written text. The audio recordings of the interview were transcribed in Microsoft Word. I removed any information that could possibly identify the participant or their associated organization to provide confidentiality. The transcribed data can aid a researcher to better code the data and draw themes from the gathered data (Zhang & Wildemuth, 2016). As an added point, it is easier to analyze written text rather than trying to find a specific part of an audio recording (Ranney et al., 2015). I analyzed and interpreted the transcription based on my understanding of the information collected during the interviews. Results from my analysis and interpretation were incorporated into the member checking process for participant analysis. I scheduled follow-up interviews for member-checking, in which I asked the participants to confirm my interpretations of the interview to validate that my interpretations reflected the participants' views and experiences. Member-checking is necessary because the researcher can impose their personal beliefs and interests on the feedback of data from the participants (Birt et al., 2016). My goal was to deter researcher bias in this study. If anything was unclear to me, I did not make assumptions about the meaning. Instead, I asked the participants follow-up questions to get clarity. If changes occur in participants' feedback during the member checking interview, I scheduled an additional member-checking interview until the participant confirmed that my interpretation of their experience is correct.

Company documents were used to validate and support the information gathered in the interviews. Multiple sources are used in a qualitative study to converge evidence that will support the explanation of the studied phenomenon (Palinkas et al., 2015). I

used company documents to provide additional insights to the perspectives of the interviewees. Document analysis requires the researcher to analyze and interpret data to gain understanding and knowledge about a topic (Polkinghorne, 2005). Document analysis is used with other qualitative research methods as a way of converging and corroborating evidence from different data sources through triangulation (Wohlin & Aurum, 2015). I reached out to the point-of-contacts in each organization, as well as the participants in this study for any documents that pertain to the security strategies used with medical devices. After member-checking was complete, I analyzed and interpreted the transcription of the data collected during the interviews and from company documents. I used NVivo 12 to organize and analyze the textual data collected in this study. The query tool in the software aided in the process of identifying themes in the collected data. Using NVivo, I was able to sort and classify data by nodes into 12 themes, which were later merged into 4 major themes.

### **Data Organization Techniques**

Data organization in my study was vital for creating themes and interpreting collected data from the views of the participants. Johnson et al. (2017b) explained that when conducting research, researchers are faced with issues on how to collect, organize, manage, and analyze data to make it meaningful to the research topic. Data collected from interviews and company documents are considered unstructured data (Varpio, Ajjawi, Monrouxe, Obrien, & Rees, 2016). Unstructured data is raw and unformatted, where important information is scattered throughout the document (Johnson et al., 2017b). Farmer, Robinson, Elliott, and Eyles (2006) referred to data organization as the

way that data is classified and organized to be more useful to the study. All documentation from this study is stored on an encrypted flash drive. The documentation includes consent forms from the participants, emails, audio recordings, and transcripts of the interviews. Consent forms and transcripts were written using Microsoft Word. Each category, such as recordings and interview transcripts, will be kept in separate folders on the encrypted flash drive.

The identity of the participants and organization names is confidential in this study. Ethical issues in qualitative research involve avoiding harm and providing protection to human subjects (Orb, Eisenhauer, & Wynaden, 2001). Study codes is an effective method that protects the identity of the participants and the organization involved in the study (Orb et al., 2001). I used study codes to protect the identity of both the organization and the participants. The study code of the participant will begin with the organization's study code to keep up with which organization the participant belongs to. Organizations' study code will begin with O1, O2, O3, and so forth. Participants' study code will be O1\_P1, O2\_P2, and so forth. Only the code names will be addressed in the study in order to keep participants and the organization anonymous. The study codes and the associated organization and participants are kept in a password-protected Microsoft Excel spreadsheet. I will be the only person with access to that Excel file. All documentation is stored on the password-protected flash drive, and the flash drive is stored in a locked storage cabinet. All physical and electronic data will be stored for five years after CAO approval, after which time all research data will be destroyed.

### **Data Analysis Technique**

During the data analysis process, I continuously went over the data collected from interviews and company documents to answer my overarching research question on strategies software developers use to protect sensitive patient information collected, sent, and stored on medical devices. Data analysis is one of the most complicated and crucial phases of a qualitative research study (Johnson et al., 2017b). Researchers examine textual data, from field notes or transcripts, inductively using content analysis to generate explanations of the study (Ranney et al., 2015). I analyzed the textual data from both interviews and company documents until I organized and converged data into four themes that supported my research question.

The textual data from interviews and company documents were categorized in such a way to provide explanations for my research topic. Constant comparison is used to repetitively analyze and identify categories in the data (Hyett et al., 2014). During data analysis, my primary focus was to analyze how internal and external influences affected security strategies from the perspective of software developers. Triangulation is a method used in qualitative research to analyze data from various sources to understand a phenomenon (Carter et al., 2014). Methodological triangulation was used in this study to cross-validate findings from multiple data sources. Data collected from various sources were used to uncover themes that would answer the focal research question of the study. Farmer et al. (2006) acknowledged that using methodological triangulation to understand the research topic will also enhance the reliability and validity of the study. Methodological triangulation adds benefits to the data analysis phase, such as strengthen

comprehension, stronger confirmation of the phenomenon's findings, and enhanced understanding of the research topic (Carter et al., 2014; Farmer et al., 2006).

Methodological triangulation was a suitable approach for analyzing data collected from interviews and company documents in this study.

I followed Johnson et al. (2017b) strategy for analyzing data, which includes compiling, disassembling, reassembling, interpreting, and making conclusions on data collected using a recursive relationship. Through the process of disassembling and reassembling data, I constructed themes from the transcribed data. Theme identification in a qualitative study is a fundamental task. Themes in qualitative research are not always clear and sometimes are abstract. Therefore, theme construction can occur before, during, or after data collection by using coding (Palinkas et al., 2015). Coding is used in a qualitative study to symbolically capture portions of language-based or visual data (Owen, 2014). Coding can be viewed as a link between collected data and their meaning (Johnson et al., 2017b). Ranney et al. (2015) discussed the multiple ways patterns can be characterized, such as (a) similarities in data collected, (b) differences in the data, (c) the frequency of patterns, (d) the patterns can demonstrate a particular sequence, (e) relations among data patterns can be displayed, and (f) explanation of what causes patterns. I used descriptive code in this qualitative study to find themes that summarized the primary topic and work towards providing an answer to the research question.

For coding, I initially had to make a selection between NVivo and Excel.

Researchers conducting a qualitative study look at special software such as NVivo, which



offers great flexibility when it comes to coding (Lewis, 2004). Microsoft Excel has features to handle and integrate various types of data as well (Niglas, 2007). Qualitative data is often composed in the form of structured text, unstructured text, audio recordings, video recordings, and so forth; analysis on this data can be completed using a range of processes and procedures (Ranney et al., 2015). When analyzing textual data, the researcher must focus on the message content, attitude of the speaker toward the message, and understand if responses were idea based (Polkinghorne, 2005). The sequential process that was used for data analysis first began with breaking down the collected data into categories. The categories were stored in NVivo. Next, the data was assembled based on similar themes found. From the assembled data, I attempted to interpret and draw conclusions. The strategy used to analyze the data in this study followed Johnson et al. (2017b) process, i.e., compiling the data, disassemble data, reassemble data, interpret data, and conclude, for analyzing data.

Fusch and Ness (2015) indicated that textual data collected in qualitative research requires preparation and organization of the data, which consist of the researcher coding to organize data into themes, condensing the codes, then presenting the findings. Themes and patterns were developed from the conducted interviews. While analyzing the transcribed interview, I kept in mind how each theme was selected, how each pattern could be perceived differently, and what each theme signified in my study. Yazan (2015) recommended constructing tables to review the transcribed interview notating information that would be meaningful to the research questions in the study. I followed Yazan's recommendation by creating tables and making notes to the transcribed

interviews. Categories were defined based on how the collected data provides insight into the research question. Using categories, I was able to highlight the strategies used by software developers to implement security measures to protect patient information in multiple healthcare organizations. Pre-coding was completed using NVivo to first review and analyze data by word frequencies, phrases, and so forth. Next, during the coding stage, data was organized by labeling nodes, which aided in understanding the relationships and underlying ideas among the codes. By reviewing the information collected for each code, themes and patterns emerged. After reassembling data and interpreting meanings, the next step was to conclude themes and patterns that were derived from the research questions (Polkinghorne, 2005). Li (2014) implied that data interpretation is based on the views of the researcher. To interpret data, Li (2014) explained that the interviewer must answer the following questions:

1. What is important in the data?
2. Why is it important?
3. What can be learned from it?

I kept those three questions in mind while interpreting data to answer the research question.

### **Reliability and Validity**

For any type of research, the researcher may ponder on ways to determine if their research is valid and reliable. After all the hard work and time spent to complete the research, it all means nothing if the outcome is invalid. The qualitative case study method uses a naturalistic approach in a real-world setting, where data collected is not

manipulated (Grossoehme, 2014). It is possible for completed research to be completely reliable but is proven invalid to the study at hand (Grossoehme, 2014). For this reason, this study included strategies to produce quality research that is both reliable and valid.

### **Reliability**

Reliability is determined by the ability to repeat the study in the same manner, and still receive the same outcome (Roberts, Priest, & Traynor, 2006). This study included strategies for selecting participants, and also used interview questions that would best increase the reliability of my study. Participant selection should be rational and purposeful to correlate to the related research questions (Cleary et al., 2014). I chose software developers who had responsibilities in the selection of security strategies to protect data collected and used by medical devices. Selecting participants who met specific requirements guaranteed that anyone involved in this study will provide valuable insights to my study. In case study research, data is collected from several data sources (Lewis, 2015).

Yazan (2015) defined triangulation as the mixing of data to cast light to diverse viewpoints. I used data gathered from interviews along with reviewing company records to triangulate evidence. I also used software and triangulation methods to search for inconsistent data that could hinder the validity of my research. Additionally, I went a step further to solidify the reliability of my research by presenting preliminary findings to participants to maintain the accuracy of my research.

Grossoehme (2014) stated that documenting research procedures throughout the research process is a way that reliability can be provided. Reliability was assured by

using documentation in my study. Using an interview protocol, I documented the sequences of the interview and analysis process: from the reasoning behind interview questions, cues that triggered other questions, the reasoning behind splitting collected data into particular categories, as well as how themes were uncovered. Yazan (2015) introduced strategies that I followed to determine whether my study justifies the validity and reliability of the research topic; these strategies included:

- Confirming that the selected respondents were knowledgeable of the subject and could provide valuable feedback.
- Searching for inconsistent data collected from the research that could possibly deem the study invalid.
- Ensuring the data collected was rich, which aided the outcome of the study.
- Using triangulation to join evidence collected from multiple sources.

Prior to selecting participants, I had a set of criteria that participants had to meet to be selected for this study. I confirmed that the data collected in this study was consistent, and any questions regarding the collected data was asked during member checking interviews. Finally, I used triangulation to join evidence from both the interviews and company documents to support the findings of the study.

### **Validity**

Validity is used as a way to determine if a study is designed well or not. Validity reassures that the results are appropriate for the intended audience (Zohrabi, 2013). In order to analyze the validity of a qualitative research study, the researcher must understand both internal and external validity. Internal validity involves the structure of

the research and determines the relationship between variables within the research (Zohrabi, 2013). Internal validity was examined during the analysis phase of the research. To determine internal validity, I matched patterns, explained how patterns were created, and addressed any opposing explanations of the data collected during research. I used NVivo 12 software to analyze data and give an explanation of the idea behind the categories for grouping data. External validity involves how much of the study can be generalized in comparison to other subjects or situations (Seltzer et al., 2017). External validity occurred in the research design phase. External validity was demonstrated by taking the findings from a case study and attempting to generalize the results. I provided external validity by collecting data from multiple sources to generalize the findings prior to drawing a conclusion. Strategies for the trustworthiness of a qualitative study involves establishing the dependability, creditability, transferability, and confirmability of the study (Grossoehme, 2014). The goal of this research study was to present trustworthy findings by ensuring dependability, creditability, transferability, and confirmability of findings from this study.

### **Research Method and Design**

Qualitative research is used to understand the meanings, concepts, characteristics, and descriptions of a particular phenomenon that can be observed (Kerkela, Jonsson, Lindwall, & Strand, 2015). Mikkonen et al. (2016) further explained that qualitative research focuses on the “what” or “how” through the discovery and exploration of participants’ views. The qualitative approach seemed more suitable to explore the research problem and to display the underlying reasons, opinions, and motivations behind

the issue (O'Cathain et al., 2013). The qualitative approach was the best approach for my study to explore participant viewpoints on strategies for implementing security measures on medical devices. I believe that using this approach allowed me to dig deeper into the trends found in security strategy selection, and present ideas for future research.

### **Research Method**

In this study, I selected a qualitative approach to explore contextual information as well as participant viewpoints and experiences to answer the primary research question. Qualitative research makes use of interviews, reviewing documents, and focus groups to discover themes that could be further researched using an inductive approach (Johnson et al., 2017b). Using an inductive approach, data analysis is the focus, and the researcher should use an emergent framework to group the data and then look for relationships (Yazan, 2015). I chose the qualitative approach because I believed using open-ended questions during the interviews would be the best approach to understand the participants' views, experiences, and motivations behind selecting specific security strategies for medical data. Due to the open-ended responses received, it was easy to turn the interview into a conversation and ask additional questions that provided additional information related to the research topic. I used an inductive approach in this study to derive meanings and relationships from participants' experiences with selecting strategies for medical device software security.

I considered conducting a quantitative study. However, to answer the research question, I would not be quantifying information. The quantitative research methods utilize surveys, interviews, and the review of other studies in order to collect numerical-

based data (Hoe & Hoare, 2013). This type of research can also be used to quantify opinions and behaviors amongst other variables. The intent of this research study was to provide insight into participants' experience in security strategy decisions involving medical devices. Statistical methods could be applied to the proposed research question in this study. Quantitative research is used when statistics will be applied to numerical data as a way to quantify a problem (Hoe & Hoare, 2013). In comparison to qualitative research, quantitative produces numerical data to quantify defined variables (McCusker, & Gunaydin, 2015). On the other hand, qualitative research produces textual data by using an exploratory approach to answer research questions (McCusker, & Gunaydin, 2015). Since quantitative research is more concerned with numerical data, instead of participants' experiences, quantitative research was not selected for this study.

Mixed-method research was also an approach that I considered for this study. A mix-method approach involves a combination of qualitative and quantitative methods to explore the research question (Kamalodeen & Jameson-Charles, 2016). A mixed-method approach is used in research that requires analysis of numerical data via experiments and surveys, and also an in-depth analysis of collected data via interviews and company records (Chan, Wang, Lacka, & Zhang, 2015). The mix-method approach can be used when a researcher is attempting to have a comprehensive look at the research problem and can derive an enhanced detailed view from using approaches found in both qualitative and quantitative methods combined (Chan et al., 2015). The mixed-method approach was not selected for this study for the same reason the quantitative was not selected, statistical analysis of the data gathered was not needed. This study was centered

on participants' experiences with medical device security strategies and company documentation on the strategies. Out of the three research methodologies, a qualitative study was the best solution to gain a deep understanding of how security strategies are selected to protect information collected, sent, and stored by medical devices.

### **Research Design**

The five qualitative approaches to inquiry in a qualitative research study include case studies, phenomenological research, narrative research, grounded theory research, and ethnographic research (Elkatawneh, 2016). To best align with the focus of this proposed study, I chose a case study design to explore strategies software developers use to implement security measures to protect patient information collected, sent, and stored by medical devices. A case study is used when a researcher wants to study a specific phenomenon, understand how decisions were made over a period of time for similar cases, and capture unique information on the subject (Tsang, 2014). In a case study, interviews are widely used as a way to support information by collecting information from participants (DiCicco-Bloom & Crabtree, 2006). By interviewing participants, I was able to understand the security strategies of medical devices from the viewpoint of the participants.

Cronin (2014) noted that a case study approach explores a phenomenon through a variety of lenses to analyze a topic through multiple facets. A multiple case study is used to explore differences and similarities between cases, which can clarify the value of findings in the study (Gustafsson, 2017). Using a case study approach in this study helped in focusing and studying external factors on security design strategies,



understanding how decisions were made for similar cases, and captured unique information on the research topic. I chose an exploratory multiple case study design because I believe it was the best way to explore current strategies software developers use to secure patient data on medical devices in multiple organizations.

Of the five qualitative approaches to inquiry, only three approaches were most appropriate for an IT problem, which were phenomenological, ethnography, and a case study approach (Elkatawneh, 2016). Phenomenological research involves examining the lived experiences of several individuals involved with a particular phenomenon (Hyett et al., 2014). Phenomenological research was not appropriate for this study because the object of this study was not to focus primarily on the participants' lived experience. For this study, company documents were needed to explore the research topic in-depth and to support the information given by participants. However, collecting company documents is not a part of the phenomenological research method. Therefore, the phenomenology approach was not selected for this study.

Ethnographic research involves the researcher interpreting and describing shared and learned patterns of practices, beliefs, and values by becoming immersed in the culture as an active participant (Baskerville & Myers, 2015). Ethnographic research was not appropriate for this study due to my conceptual framework, which analyzed external influences that affect software developers' security strategy decisions. The ethnographic research design was not selected because this study is not based on cultural experience alone. This study explored how other influences, in addition to cultural influences, such

as social, institutional, and economic influences, affect security strategies software developers use to protect medical device data.

This study included data from multiple sources, i.e., interviews and company documents, to achieve data saturation. To reach data saturation, the researcher must (a) select respondents who are knowledgeable of the subject, (b) endorse that data collected from documents and interviews are rich, and (c) join evidence using triangulation to support conclusions made in the study (Yazan, 2015). Saunders et al. (2017) stated that a researcher would know when data saturation is near completion due to the increased redundancy of data collected from participants. To facilitate data saturation, the same set of questions along with impromptu probing questions to fully understand participants' perceptions was asked in each interview (Robinson, 2014). To obtain data saturation, I tracked and triangulated data from interviews and company documents until new information was no longer generated from the interviews. Additionally, I collected company documents from the point of contact that related to security strategies for medical device data security. When no new information was presented during the triangulation of company documents and interview data, I knew that I had achieved data saturation.

### **Strategies for Trustworthiness**

**Dependability.** In this study, I (a) followed the steps given in the interview protocol (see Appendix B), (b) analyzed results through member-checking, and (c) utilized triangulation of all collected data to provide dependability. Dependability refers to the stability and consistency of the findings in the research study (Zhang &

Wildemuth, 2016). For dependability to be provided, the instrument (i.e., the researcher) has to be consistent during the observation and analysis of the data (Zohrabi, 2013). The interview protocol was developed to provide consistency during the interview process amongst participants. Any variation from the interview questions was included in the transcribed data of the interview. Member checking was used to ensure that the conclusions drawn from each interview were only from the perception of the participants. After the member checking interviews were complete, data analysis occurred to verify consistency in findings between examination. Additionally, I triangulated the data by using secondary data sources (i.e., company documents) to support findings from the primary data source (i.e., interviews). Triangulation promotes data validation by collecting data from multiple data sources on the same topic (Carter et al., 2014).

**Creditability.** Nebeker et al. (2016) stated that the creditability of research could be achieved by selecting participants who meet specific criteria for this study, i.e., years of experience, job role. Creditability is established when data collection and data analysis procedures are conducted in such a way that any relevant data has not been excluded from the study (Bengtsson, 2016). Often, participants are hesitant about sharing information in research for fear of backlash. Providing confidentiality and anonymity will help participants be more open with the data shared in the study (Bengtsson, 2016). For this case study, software developers whose primary focus was on the security aspect of software within multiple software companies were interviewed. Member checking was used to confirm my understanding of the data collected. Member checking is used to test the interpretations of participants' data to enhance the credibility of the data collected

(Pitts & Miller-Day, 2007). The open-ended interview questions allowed participants to share their experience with software security strategies for medical devices.

**Transferability.** This study included descriptions that explained the procedures that took place in this study, which will allow the findings of this study to be reproducible. Transferability refers to how applicable the findings of this study would be to other groups or organizations (Grossoehme, 2014). A vital strategy to establish transferability in a research study includes choosing a representative sample (Saunders, 2012). Working with the point-of-contact from each organization, I was able to select a diverse sample of participants who met the criteria for this study. Doody and Noonan (2013) noted that researchers could not directly prove that their research would apply to other contexts, situations, times, or population. However, the researcher should provide enough data that readers of the study can make informed decisions on the transferability of findings from the study (Doody & Noonan, 2013). The research design for this study was a multiple case study, which took place in more than one organization that deals with medical device security. This study could be used in other organizational settings to aid in generalizing the results.

**Confirmability.** Confirmability refers to the objectivity or neutrality of data collected in the study (Ryan-Nicholls & Will, 2009). Grossoehme (2014) argued that researchers have their own values, which is sometimes impossible to separate from observation. However, the researcher's values should not overshadow the participant's views in the study (Grossoehme, 2014). In order to obtain confirmability in this study, I conducted a confirmability audit. The confirmability audit was completed during the

member checking process to assure that my analysis of the interviews was strictly from the participant's experience. Triangulation of data from multiple sources is an additional way of checking the data collected and providing support to the findings of the study (Varpio et al., 2016). I used methodological triangulation to review and confirm results from interview data through company documents.

**Data saturation.** This study consisted of analyzing data collected from semi-structured interviews and company documents to achieve data saturation. Bengtsson (2016) suggested that in confirming the creditability of a study, data collection and analysis should be conducted in a way that any relevant data is not excluded from the study. Data saturation has been reached when no new evidence is emerging from the data collection process (Robinson, 2014). I used in-depth opened ended questions to gather information from software developers with various levels of experience in multiple organizations. Fusch and Ness (2015) concluded that failure to reach data saturation in a qualitative study has an impact on the quality, creditability, and validity of the study. I continued to conduct interviews and follow-up member checking until no new data emerged. During data analysis, the repetition of data found and the failure to identify new themes informed me that the study had reached data saturation.

### **Transition and Summary**

Section 2 included information on reasons behind participant selection, research methods, data analysis techniques, and how reliability and validity were sustained in the study. The information found in this section provided the background for conducting a qualitative case study to explore strategies to provide security measures for medical

devices. Information on the security strategies was gathered through interviews with software developers who had various levels of expertise on the security aspect of medical device software. Additional information was gathered by reviewing company documents and correlating documentation with interview responses. Section 3 will consist of an overview of the study, along with the findings from the data collected. Section 3 includes information on how the research from this study can apply to professional practice and potentially lead to social change. Additionally, section 3 includes recommendations for both action and further studies, as well as reflection, summary, and conclusion of the study.

### Section 3: Application to Professional Practice and Implications for Change

Section 1 reviewed the foundation and overview of the study. Section 2 assessed the techniques and methods used in the study to ensure quality research. Section 3 builds on Section 2 by reflecting on the overview of the study and examining the findings from the participants in my study. In section 3, I examine the presentation of the findings, application to professional practice, and the implications for social changes. Additionally, I review recommendations, further suggestions, and personal reflections.

#### **Overview of Study**

The purpose of this qualitative exploratory multiple case study was to explore strategies software developers use to implement security measures to protect patient information collected, sent, and stored by medical devices. Data for this study came from interviews with software developers and company documents from three software companies in the Baton Rouge, LA, area. The findings showed issues, strategies, influences, and considerations used by software developers to implement security measures to protect patient information when using medical devices.

#### **Presentation of the Findings**

This section presents the findings and themes that were formed throughout the study. The focus of this study was to answer the overarching research question: What are strategies that software developers use to implement security measures to protect sensitive patient information collected, sent, and stored on medical devices? The answers found in this study may aid in helping IT software developers forge viable strategies that incorporate external factors outside of technological aspects, such as user influences,

third party authorization, legal liabilities, and monetary factors. For this study, I collected data from multiple sources. I conducted interviews over the phone, which allowed participants to take calls in a comfortable setting and also increased the flexibility of the participant's time. Each participant provided detailed responses to the demographic and interview questions. I performed member checking to establish the accuracy and validity of my interpretation of the data collected from the interviews. Furthermore, I used company documents as another source to reveal valuable information to the study, which included strategies used to protect against security vulnerabilities and how decisions were made. By having company documents as an additional source of data, triangulation occurred, which was a way of assuring the validity of data collected through interviews.

Prior to the data analysis process, I transcribed the interviews from the participants and imported the transcriptions and company documents into NVivo 12 software. The textual data from interviews and company documents were organized in such a way to emerge themes from the findings. The findings from the participants were analyzed and converged into themes based on the conceptual framework for this study, the SST. I involved three organizations in this exploratory multiple case study with a total of 10 participants. Participants selected for this study all worked with software development for medical devices and were in three roles: developer, development lead, or technical architect. Participants' experience with medical device software ranged from 2 to 26 years working with patient portals, radiology machines, rehabilitation robots, kiosks, telemedicine carts, and so forth. Six of the 10 participants believed they were



knowledgeable of the interrelation of cloud security and medical device technology, while all believed they had some insight into the security of these devices. Participants' code names for the purpose of this study was set up as OrganizationCode\_ParticipantCode, for example, O1\_P1, which stood for participant 1 from organization 1.

Initially, 11 themes emerged from the data based on the frequency of keywords, the points made by the participants, and the analysis of company documents. The 11 themes were drilled down and groomed into four primary themes for this study. The four themes were as follows: (1) securing medical device data, (2) social influences on medical device, (3) establishing standard policies for medical device security, and (4) factoring costs for medical device security. From the interview transcripts and company documents, I was able to determine if the external factors discussed in the SST theory influenced medical device security decisions (see Table 1). The aspects of the SST found to influence software developer's decisions regarding medical device security included social, institutional, cultural, and economic influences.

Table 1

*Themes for Extensive Collaboration is Critical*

Major theme and influences	Participant		Document	
	Count	References	Count	References
Social shaping of technology				
Social influences	7	46	5	29
Institutional influences	9	22	6	37
Economic influences	10	54	4	22
Cultural influences	10	27	3	28

**Theme 1: Securing Medical Device Data**

The security of medical device data was the first theme that emerged from data analysis. I found that software developers' perception of security strategies only partially affected security adoption within an organization. There are many challenges and vulnerabilities that need to be addressed in a healthcare organization due to rapid technological changes. These rapid changes to technology stem partially from the external factors found in the SST theory, such as legal liabilities, regulatory liabilities, recovery costs, users' wants and needs, and so forth. There are several recommendations to overcome the challenges faced during security strategy implementation. As noted by Brand (2017), proper analysis of current influences in connection with medical device security strategies would abet software developers in limiting cybersecurity defects. Following Brand's concepts on proper analysis, aspects of the SST theoretical framework were present in each theme in this study.

Table 2

*Frequency of First Major Theme*

Major theme	Participant		Document	
	Count	References	Count	References
Securing medical device data	10	58	7	43

Security is a leading factor in the success or failure of medical devices/software. All it takes is one time for a security breach to be vast enough to diminish the reputation of an organization and put patients' personal information at risk. Multiple participants indicated how data breaches could quickly diminish the reputation of any organization. Once trust is lost in an organization's product, rebuilding the brand could be the cause of an organization going bankrupt. Having security strategies in place to rectify the situation in the event something goes wrong immediately builds medical staff and patients' trust in the product. Participant L\_P1 indicated that security strategies are dependent on the type of software and hardware used, as well as the business needs of the organization. Security strategies discussed included anticipating potential threats, learning from the past, consistent monitoring of the current system, and the usage of encryption. Company documents from organization L outlined the costs associated with the various services provided to healthcare organizations.

All 10 participants reported the importance and necessity of security analysis during initial requirement gathering, throughout the development lifecycle, and continuing through the maintenance phase of the medical device/software. Study findings from two company documents also pointed out that implementing security

protocols outweighed meeting all of the required features for medical devices (see Table 2). Participants I1\_P2, I1\_P3, and L\_P3 worked typically with medical staff directly and asserted that reducing security concerns for customers shifts medical staff focus to the patient. Seven of the 10 participants pointed out that the majority of the decisions for security strategies were from federal regulations. Users and medical staff hesitance to use medical devices were due to a lack of trust to truly secure patient data, as well as reluctance to change. A document on presenting medical devices and software to potential clients indicated that the word security should rarely be used, and more focus should be placed on the benefits of the device/software. Three participants indicated that during demos of new devices/software, they avoided discussing security in-depth. They found that attempting to explain security measures and the reason for specific methods raised concerns from nontechnical resources, which diminishes trust.

There were several security strategies described by participants from each of the three organizations that aligned with security strategies found in the literature. Most medical apps and devices are designed using a problem-driven approach instead of using a security-driven approach, which ultimately could increase cyberattacks in the future (Khera, 2017). Participants from each organization reported in interviews that organizational rules and stakeholders' decisions affected the decisions for security strategies. Participant I1\_P1, who had 16 years of experience with his current organization, explained how security and design decisions evolved in the organization. Participant I1\_P1 further explained how initially decisions on security strategies were made by stakeholders alone, and they only accounted for the cost of those strategies. It

took having a major security breach due to the new system not being compatible with the main legacy system for stakeholders to realize the need for technological expertise.

Participant L\_PL9 indicated that he had encountered times where his development lead and stakeholders took user requests for new software as a Christmas list and made promises to deliver without considering the actual impacts to security these additional changes could have. Company documents supported the participant claim by acknowledging that (a) insecure configurations, (b) lack of strong testing for process controls and system configurations, (c) lack of basic network security protection, (d) segmentation, and (e) issues that come with maintaining legacy systems were not adequately analyzed in the past leading to security vulnerabilities.

Participants in this study acknowledged that in their organization, they currently use or have used a legacy system that either stores data or manipulates data for transmission. Legacy systems must be continuously maintained to keep up-to-date with current technology. Participant I1\_P1 discussed how the legacy system used in his organization had been analyzed to determine what new software should replace the legacy system, a significant factor in this decision was the cost to replace versus the cost to maintain. Participant I2\_P2 discussed how keeping the new technology and current security measures compatible with the legacy system is a headache. At the time of this study, organization I2 was still using a legacy system from 20 years ago. Participant I2\_P1 explained how a simple security patch that occurred two years ago by Microsoft caused the user interfaces of their kiosks to revert to a Windows 95 interface. That patch was not compatible with the encryption methods used in the legacy system, which caused

user passwords and other personal information to be displayed on the screen in plain text. Serban (2016) stressed challenges associated with medical devices that still used legacy systems: (a) compatibility, (b) security, and (c) the cost to update. Due to the challenges of updating and maintaining legacy systems, organization L stopped working with legacy systems and focused on creating new software. Using new software over a legacy system has the benefits of reducing costs over time, fewer risks with updates, and have the latest technology for potential customers.

It was uncovered that organization I1 and I2 utilized access control mechanisms to provide security for access control that is compatible with their legacy systems. Furthermore, organization I2 used Salesforce Health Cloud for the user interface that connects with their legacy data management tool. Company documents from I2 supported how access control is a built-in feature of Salesforce that only needs to be appropriately configured. Salesforce has user permissions and access controls such as organization-wide defaults, role hierarchy, sharing rules, and so forth (Salesforce, 2017). The access controls mentioned above provides each user with a certain level of access depending on their profile and their role in the company (Salesforce, 2017). Participant I2\_P3 indicated that it is rarely reported when a user has too much access to the system, but often get grievance from users not able to see required data. Correct methods for identification and authentication are just as crucial as other security measures implemented to protect sensitive data. Software developers can start by implementing enhanced password requirements, which could offset threats from passwords easily guessed, or any form of password attacks on the software (Mahmood, Ning, Ullah, &

Yao, 2017). Researches such as Yang, Lo, Liaw, and Wu (2017) placed emphasis on adding to password enhancement requirements by requiring two-factor authorizations as an additional means of securing identification and authentication. Participant L\_P1 acknowledged the lack of access controls found within his organization. He stated that his organization failed to recognize fundamental issues, such as password strength. Participant L\_P2 supported this by adding that the organization is so focused on being approved for the market that some basic standards are overlooked.

Due to the threats of hackers waiting to uncover potential vulnerabilities, encryption was mentioned as a possible solution to minimize security vulnerabilities found in both the software and the transmission process. Participant L\_P3 pointed out that organization L is using older encryption methods that should be reviewed; however, security gaps have yet to be found with them. Organization I2 used Salesforce as the central system used by patients and medical staff, which allows seamless desktop and mobile device usage. Patient data is stored in a master data management (MDM) hub and syncs with Salesforce. The MDM is used as a central location that improves the quality of data while transmitting and syncing data with various software. Participant I2\_P1 discussed how transmission of data has to be secured on multiple levels. Active and passive threats are concerns that can arise during the transfer of data. Passive threats such as eavesdropping allow a hacker to intercept data being transmitted (Alaba et al., 2017). Data modification and alteration to the way the system functions are considered active threats (Kumar, Kaur, Kaur, & Singh, 2016). Participant I2\_P1 believed that real hackers do not need access to the user interface to hack information, but only need a tool

to intercept data in transmission. Company documents list five common encryption types that should be chosen from. The document further described other security measures to enhance security measures during data transmission. Along with using antivirus software, participant L\_P1 asserted that encryption methods for data transmission, strict encryption and decryption methods for databases, and virtual private networks (VPN) should all be used concurrently as a means of security.

Security mechanism choices are also influenced by institutional or cultural dynamics, i.e., internal values, strategies, and resources of the healthcare organization. Cavusoglu et al. (2015) discussed how technical controls should be the first line of defense to detect security threats in systems. Technical controls are often used as a “set it and forget it” type control and is used to identify device malfunctions promptly. Company documents for organization I2 confirmed that during updates, some technical controls were forgotten, Participant I2\_P2 argued that by overlooking something as small as a configuration checkbox during analysis could expose sensitive data or make the system not work as expected. Fault tolerance safety measures should also be used in addition to technical controls just in case a malfunction occurs that goes beyond technical controls limitations.

In any hospital or doctor's office that uses medical devices, there are many varying manufacturers for the various equipment and software used. In the case of using multiple devices that have different software standards, software developers must keep in mind that if legacy systems are not updated to the latest security measures, vulnerabilities can be exposed over the network. Sometimes unintentional issues occur in the system.



Unintentional issues to security were encountered by participant L\_P3 while working on a telemedicine cart for nurses. During a shift while passing out medication, a nurse plug in her cell phone to the cart via USB to charge. The telemedicine cart took the phone as a threat to patient data and shut down the cart when the phone sent an alert to trust the computer. This was perceived as an unintentional social threat to the system, but in the case of an actual threat, the cart shut itself down. Researchers at the Department of Health and Human Services (n.d.) explained how users could cause unintentional issues with a system due to honest mistakes or even a degree of negligence. MacKenzie and Wajcman (1999) created the SST theory to illustrate how technological advancement, execution, and utilization are affected by social factors. The SST consist of four external factors that each affect medical device design strategies. Findings from the data provided by several participants in the study were consistent with the conceptual framework SST relating external factors to software design choice considerations. Of the four factors discussed in the SST theory, social influences were substantial in evaluating security measures for medical devices.

## **Theme 2: Social Influences on Medical Device Security**

The second theme that emerged from analyzing interviews and company documents is the social influences that affect design choices for medical device security. In correlation with the SST theory, external factors such as user impacts and third-party pressures link to the social influences that affect medical device security. During software development, human factors and influences should be considered in the design. Researchers such as Latif, Othman, Suliman, & Daher (2016) advised using a user-

centered design approach in medical device development. This approach will allow participants to be involved in preliminary requirements and design changes throughout the development process. User interactions with medical devices are sometimes in opposition to the developers' and manufacturers' plans for the intended use, which is why usability testing is needed to evaluate improvements needed for user performance and satisfaction. Third-party influences include the individuals (i.e., healthcare providers, medical device users, and hackers) who may not have direct connections with the medical devices. It is also found that some non-sensitive data is given to third-party agencies unknowingly. When users, especially on mobile devices, give consent for third-party access to medical apps, they sometimes are unaware of the endangerment to data protection (Hall and McGraw, 2014).

Table 3

*Frequency of Second Major Theme*

Major theme	Participant		Document	
	Count	References	Count	References
Social influences on medical				
Device security	7	46	5	26

Oguz (2016) emphasized how outside stimuli and the decision-making process have a direct effect on technological changes. Participants from Organization L and I1 emphasized how outside influences molded their decisions for design strategies (see Table 3). Three participants from organizations L and I1 also conferred that user considerations, ease-of-use, specific features, regulations on medical software, and so

forth, all played a role in choosing design strategies. Contrarily, participants from organization I2 believed that outside influences do not affect their design choices. Participants in organization I2 beliefs on technological changes aligned with researchers, such as Papageorgiou and Michaelides (2016), who believed changes in technology is independent of any form of social influences. Participant I2\_P1 alleged that his organization does not conduct user acceptance testing to ensure they chose the correct security design; final security decisions come from stakeholders and executives.

A design constraint of developing medical devices for various users is the simplicity of the device/software. The software needs to be simple enough for an 80-year-old with limited technology proficiency versus a teenager that uses mobile devices on the regular. Six out of 10 participants believed that the user's age range was an insignificant factor when selecting medical device design choices. Three participants discussed how they had encountered medical professionals who were against a new system being introduced due to being more comfortable with an older system. Five out of 10 participants from 2 of the companies have experienced medical software failing user acceptance and had to change designs to meet user expectations. Participant I2\_P2 pointed out that having to alter user interfaces could affect validation rules and security features if items were removed or added on the user interface. Company documents did indicate that after the development process began, stakeholders have had to ask for some software features to be redesigned due to security issues that occurred. For this reason, Participant I1\_P1 believed that using a panel of SMEs in the initial phase of analysis would eliminate failure during development. A company document also acknowledges

that having SMEs designated to each project positively impacts the quality, efficiency, sustainability, and security of the software developed. Participant I1\_P1 perspective on SMEs aligned with company documents by indicating that having a panel to analyze, discuss, and grade new software/hardware would change the views on various design perspectives.

Participant L\_P2 discussed issues involving end-users not utilizing the device as designed, which revealed security gaps in the system. User impact on security design was minimal for the participants in this study, with only 4 of 10 participants stating that user influence was a factor. Salesforce Health Cloud ensures patient data and correct utilization of the system by making sure users only saw what was needed to perform their duties. Salesforce has several levels of access controls that determine who sees what in the Salesforce application (Salesforce, 2019). External users', i.e., patients, access to the system also affected how security is set up for medical data. I1\_P1 indicated that at one point in time, patient medical data did not belong to the patient, but was solely the right of the medical organization. Even if the patient wanted to transfer, it was up to the organization, and they were not obligated to share medical information. Changes to HIPAA laws, along with technology updates, allowed users to have more access to their medical information from any hospital, doctor's office, or device with network access, but it caused risks with data being transferred over the network. Security threats to data being transmitted over the network were the reason behind participant L\_P1 arguing on the importance of using a multi-layer architect to enhance the security of medical devices/software. Having and investing in defense mechanisms such as SSL and

encryption gave users the access required to data while enforcing desired security measures.

Due to the money involved with selling patient data, hackers rely on undiscovered vulnerabilities in the system to capitalize on (FDA, 2015c). Participant I2\_P3 asserted how sometimes developers' input seem to be heard only after the initial release of the software. Feedback from users exposes some issues that, if adequately analyzed, could have changed the design choice selected during the analysis phase. Only 2 of the 10 participants ever had any experience with hackers, while 5 out of 10 participants were aware if their organization had any preventative measures against hackers. Two company documents provided insight on how hackers target healthcare organizations and how using the cloud or personal devices is a concern to medical organizations. Organization L produced an incident response plan, which included issues that occurred in the past, the way it was handled, multiple ways the situation could have been better handled, and suggestions for the future. The booklet had 17 scenarios that have occurred, ranging from security breaches; to the system shutting down; to issues with inaccurate data. Participant L\_P1 elaborated on the company document by explaining how a person that is on-call for security issues has that guidebook, which covers most scenarios and directs that person on the next step to take towards mitigating the problem.

Researchers, such as Faiella et al., 2018, discussed the importance of having a security team composed of people in the company with various levels of expertise and various backgrounds. Participant I1\_P1 reinforced the benefit of having a team for design decisions by discussing how their organization has a panel of SMEs that provide

input for specific areas of expertise, i.e., hardware, software, security, specific department heads, and so forth. This same team is called when problems occur in the system to come up with the best possible solution. Researchers such as Klonoff (2015) discussed that a security team should follow the CIA (confidentiality, integrity, and availability) Triad as a means to safeguard data. Participant I1\_P3 discussed a scenario on how access controls were not set up correctly, which led to medical staff being able to see a list of all patients treated and their treatment on a particular date. This was a violation of keeping data private but was fixed within a few hours. This consequently led to the decision for organization I1 to create a security team in order to ensure security.

Some development plans have straightforward solutions, but for larger projects, the solution requires more analysis. Security teams were used by 2 of the 3 companies. For the third company, the developers and testers circled back as the security team to catch threats in the design. As indicated by Participant I1\_P2, it was hard as developers to test not only the functionality of software but also the security. The two companies that had a dedicated team for security, whether in-house or third party, both saw fewer threats with the release of software updates or new medical devices. Another factor revealed that relates to social influences on medical devices is the state of the current industry. Stakeholders try to take into account the current trends versus the actual drivers behind those trends. Company documents pointed out that drivers in the current industry included making end-users apart of the solution, being driven by cost and efficiency, or merely ensuring compliance to both organizational and federal regulations.

From the literature, the social shaping of smartphone technology is a prime example of how changes and added features to smartphones are influenced by user wants and by features that follow the latest technology trends (Lee & Soon, 2017). Smartphone technology is one of the most popular long-lasting technology where features are enhanced based on external influences. Some smartphone users store everything from personal information to credit card information on their devices. Enhancing smartphone innovation has led to an increasing need for updated security. Likewise, innovative thinking and external influences affect advances with medical devices, as well as the necessary security for medical devices.

### **Theme 3: Establishing Standard Policies for Medical Device Security**

The third theme that emerged from analyzing interviews and company documents was establishing standard policies for medical device security. Two external factors from the SST theory emerged in this theme: institutional influences and cultural influences. Federal guidelines fall under institutional influences, whereas organizational guidelines fall under cultural influences. Institutional influences include regulatory implications, which are defined policies for medical device manufacturers provided by federal organizations such as the FDA and FCC. Not following or understanding regulatory pathways could lead to the medical device organization facing legal liabilities, fines, recalls, and so forth. Cultural influences reflect the core values of the organization based on factors such as beliefs, assumptions, perceptions, thoughts, and feelings (Matko & Takacs, 2017). Every organization has its own culture, which is built through

interactions, rewards, management, and other unspoken or unwritten rules followed when working together.

Table 4

*Frequency of Third Major Theme*

Major theme	Participant		Document	
	Count	References	Count	References
Establishing standard policies for medical devices security	10	49	9	65

Very few organizations are registered with the FDA due to the category their particular medical device software falls in (FDA, 2019). Participants from all three organizations, in this case study, stated that their organizations' regulations are similar to the federal laws for medical software/devices. There were four documents obtained from the organizations containing federal regulations that were both mandatory and optional for medical device design. All participants agreed that outside of security, federal regulations had a significant impact on the design process of medical devices (see Table 4). Participant I1\_P3 further iterated how their organizational guidelines are updated quarterly to make sure that their software/devices meet federal guidelines. Researchers such as Weininger, Jaffe, and Goldman (2017) blamed security concerns with patient data in medical devices on the lack of federal guidance issued for standard applications. Participant L\_P1 agreed with the researchers by stating how federal regulations need to be reevaluated. He further stated how organizations are able to slip through loopholes found in federal policies to focus more on revenue over meeting guidelines.



Serban (2016) emphasized that there are three challenges associated with medical devices related to federal regulations, which included: (a) compatibility, (b) safety and effectiveness, and (c) the overall cost. Members of the FDA and the FCC have worked together to define policies for medical device manufacturers as a guide on the regulatory requirements for medical device technologies, especially since all software does not have to be gauged by federal agencies (FDA, 2019). Federal regulations are usually stricter than organizational regulations, but not always followed. Six out of the 10 participants stated that federal regulations were evaluated during the analysis phase of medical device/software development. All participants agreed that federal policies have a strong effect on design choices. Even though the FDA has stricter guidelines for medical devices as opposed to the guidelines for medical software, this strictness does not apply to the device updates. Participants L\_P3 and L\_P1 reported that their company would add to existing device functionality or make a next-generation version of the already approved device. Using this approach, medical device organizations can avoid having to go back through all of the FDA checkpoints for the device to be released to the market. To be considered an update, the new and improved device has to have the same hardware and basic functionality as the predecessor.

Due to security attacks, an organization could be faced with lawsuits because of (a) data breaches, (b) profit loss, (c) recovery cost, and (d) fines imposed by federal agencies (Zeadally, Isaac, & Baig, 2016; Camara, Peris-Lopez, and Tapiador, 2015). Participant L\_P1 asserted that as far as his knowledge goes with federal regulations, risk management is not thoroughly discussed; it is up to the organization to provide risk

management during the development lifecycle. Not only should organizations offer risk management for medical devices, but developers must understand what influences design choices and organizational decisions when implementing a system. Empirical research would aid in identifying problems or questions through observation, study significant decision points, derive conclusions based on research, performs tests using several decision points, and evaluate the outcome (Wohlin & Aurum, 2015).

HIPAA privacy rules are very strict on who can access a system, who can view what records, and who should be making changes on patient's electronic health records. However, these rules do not always apply to all medical software (Kruse et al., 2017). Participant L\_P1 pointed out how HIPAA laws do not process safety compliance for medical devices, but to mitigate risks, the organization has internal compliance procedures written in the organizational policy. Participant I1\_P1 indicated how HIPAA policies made significant changes in the way patients can control their data. A company document, *HIPPA Privacy Rules Series 7*, facilitated the constraints of medical data prior to the law being change, data was thought to be owned by each hospital and/or doctor's office. According to the document, HIPAA laws required patient data to be readily available and easier to transfer between medical organizations as long as patients signed off. Participant I2\_P1 also acknowledged how HIPAA compliance is not required for all of the software developed in their organization; however, management makes it a practice to incorporate HIPAA guidelines when creating medical device/software.

In alignment with data collected in the study, scholarly literature provided insight on how organizational culture and software developers' viewpoints can be influenced by

each other. Software developers' views on security adoption can strongly affect the security design choices used in keeping medical data safe (Hall & McGraw, 2014).

Software developers' viewpoints on security strategies are typically formed by organizational culture. The culture reflects the core values of the organization based on factors such as beliefs, assumptions, perceptions, thoughts, and feelings (Matko & Takacs, 2017). Organizational culture is learned, and it continues to evolve as software developers gain experience and work with others that have various levels of expertise.

Participants from two of the three organizations believe that users and outside influences affect security design choices. It is a part of their organizational standards to bring extraordinary service and bridge the needs of users with the software requirements when it comes to analysis. However, participants from the third organization indicated that stakeholders make the ultimate decision regarding design strategies, security mechanisms, and so forth. This means that software developers' solutions focus on solving a problem in a particular way that is mostly defined by someone else already. Two of the three organizations have a designated security team, while the third organization handles security issues throughout the development phase and from user feedback. The way participants in each organization handle security scenarios were based on the culture of the organization. Six participants shared how their current organizations' culture differed from that of organizations they were previously employed with, and how they were able to bring prior learned experiences to their current organization. Participant I2\_P3 claimed that learning from past mistakes, current trends,

social impacts, and possible threats could influence the way the security of the system is enforced

Matko and Takacs (2017) defined organizational culture as the normative glue that connects the belief systems of an organization and institutionalizes the perception of employees of that organization. Organizational influences on medical device security strategies tie in with the organizational culture. A lead developer in organization I1 discussed how there is a panel of subject matter experts that take a vote from all points-of-views. On the panel are the medical staff that would be using the device, the necessary department heads, developers, testers, and any other personnel that are deemed essential for the device development. Members of the panel take a few days, even weeks, to hash out and vote for or against new hardware and software. A requirement of this panel is to ensure that new strategies/devices fit with the organization's mission in producing new devices/software. This requires research because two important pieces of information that come out of the meeting are the usability and benefits of the new hardware/software versus the overall security. Participant I2\_P1 argued that when it comes to new projects, as the development lead, he gives his input, but the ultimate design decisions come from stakeholders. This does not mean that the stakeholders' decisions are the most suitable; however, decisions in organization I2 are handled as a dictatorship for decisions over a democracy. A company document on medical device development planning indicated that it is normal for that organization to utilize a team to create a development plan in order to access multiple perspectives from varying levels of

expertise. Participant L\_P1 has worked for companies that had each voting style for new software, i.e., team input or selected stakeholders making all of the decisions.

#### **Theme 4: Factoring Costs for Medical Device Security**

The final theme that emerged from analyzing interviews and company documents was factoring costs for medical device security. The final theme aligns with the classification of economic influences found in the SST theory. Economic influences on business decisions for medical device organizations occurs whenever that decision is affected by any monetary factors, such as constraints and budgets. Software developers' decisions on security strategies for medical devices are influenced by a wide variety of impacts; however, next to security, the cost is always a major factor for stakeholders. Technology impacts economics just as much as economics impact technology (Sametinger et al., 2015). To get medical devices on the market, medical device manufacturers have to overcome barriers such as regulatory standards, new and complex changes to technology, and quality in order to sell their products at a reasonable price to compensate the development efforts (Tibau et al., 2014; Diaconu et al., 2017). However, while overcoming the mentioned barriers, the medical device manufacturer must stay in budget.

Table 5

#### *Frequency of Fourth Major Theme*

Major theme	Participant		Document	
	Count	References	Count	References
Factoring costs for medical device security	10	54	4	22

All participants from all three organizations agreed that economic factors and social influences were the driving force behind medical device design choices (see table 5). Company documents supported the notion that budgets for various medical device/software projects were calculated based on society's interests or needs, organizational decisions, and required federal regulations. The various influences on the organization's projects align with the SST theory in which technological strategies are influenced by external factors. The primary goal of all three medical devices/software organizations in this study was to design, produce, and release products as soon as possible to see a return in revenue. Both organizational regulations and federal regulations influence economic decisions regarding medical device security.

Economic influences were mentioned in some form by all participants in the study. Company documents from organization I2 presented the estimated initial costs plus maintenance cost for a 5-year contract implementing software. The document further explained how hospitals and doctor offices could choose from a variety of device/software types that best suits their needs for patients. In-house versus using a Software-as-a-Service (SaaS) platform differed as much as \$500,000 in yearly fees. Economics was only referred to by participants in a negative light when discussing sticking to a budget for the sake of a project. However, when it came to security, all participants were in agreement that cost should not be spared. Six of the 10 participants believed that federal regulations caused increases in the budget to accommodate general requirements. It was either a pay now or a pay later factor that influenced business decisions.

Participant I2\_P1 believed that when it comes to security, the budget is never a factor because the security has to be in place regardless. Participant L\_P3 negated participant I2\_P1 by indicating how some organizations have purposely skipped some federal regulations to save money. Three of the 10 participants discussed how sometimes features were removed from project plans for the sake of time and budget to focus more on security. The ultimate goal is to design and extend the lifetime of the software. All participants from all three organizations were in agreement that economic factors and social influences were the driving force behind medical device design choices. Company documents supported the notion that budgets for various medical device/software projects were calculated based on society's interests or needs, organizational decisions, and required federal regulations, and so forth.

**Organizational budgets.** Organizational budget was a sub-theme that surfaced during data analysis and aligned with constraints and economic influences from the SST theory. In my review of the organizational documents, participants from organization I1 confirmed that to make the most out of organizational budgets, human resources, physical assets, and other resources should be allotted to be used efficiently and optimally. The budget projected by an organization includes the cost to complete a project in a specified timeframe. The budget also consists of fixed and variable costs, which could be the cost of developing the software plus additional costs associated with missing project deadlines for delivery. Other factors on the budget could include the cost of labor, licenses, travel, and so forth. The production of medical devices can cost anywhere from \$10 million to \$20 million for both development and testing (Van Norman, 2016). Software developers

and leaders of medical device organizations face pressures for cost containment when selecting security mechanisms for medical devices (Johnson, Belin, Dorandeu, & Guille, 2017a). Throughout data analysis, it was found that budgets could make or break design decisions.

Regulatory standards, technology changes, and product quality are some of the barriers medical device manufacturers have to overcome to get medical devices on the market (Tibau et al., 2014; Diaconu et al., 2017). Proper research during initial analysis provides software developers and stakeholders with insight on the economic implication their security design choices add to the development process. However, the final decision on security measures is not always up to the software developers. Participant I2\_P1 iterated that he gives his opinion as a technical architect on projects, but it is not always taken into account when stakeholders are making decisions on a design choice to use. Participant I2\_P2 further iterated that he wished that the development team could put together a proposal for various design choices to present, then stakeholders pick from the solutions given. Participant L\_P1 elaborated on how a design choice was rejected a third of a way into development due to issues with the legacy system; poor initial analysis led to major profit loss.

There are many reasons why stakeholders in medical device organizations could decide against specific security measures, i.e., costs, overall value. Researchers such as Fernandez-Aleman et al. (2015) stated that the budget sometimes limits the security measures for healthcare data. Participants I1\_P3, I2\_P2, and L\_P3 all have worked on projects that were both over budget and had missed deadlines for delivery. Participant



I1\_P3 elaborated on how one project was \$100,000 over budget due to underestimating when it came to equipment, cost estimates, and issues from the legacy system that was not accounted for. All participants agreed for different reasons that the budget is essential to the scope of the project. Money should be invested in the infrastructure of the organization to make sure that hackers cannot intercept sensitive data being transmitted. Software bought may be expensive due to the built-in security, amongst other desired features. For example, participant I2\_P2 indicated how the Salesforce Health cloud implementation cost upwardly of \$80,000. However, the built-in security features associated with the system were worth it. Less time was spent on security, and more time was allotted to enhance features for users.

**Federal budgets.** Federal budgets were another sub-theme that surfaced during data analysis and aligned with constraints and economic influences from the SST theory. Participant I2\_P3 made a critical statement that getting a product to market is hard in general but getting a medical device to market is even harder. Aligning internal analysis with federal regulation within an organization is pivotal for the successful launching of the medical product. However, if the product fails to meet regulatory requirements, then that means the organization has to spend more money to meet the guidelines. As mentioned by Chen et al. (2018), some companies choose to enhance medical devices that have already passed FDA and HIPAA standards. Enhancements to a previously passed medical device allow for new features to be placed on the market expeditiously, rather than creating a new device or software from scratch. The enhancement route skips

steps in having to have the medical device or software evaluated and can potentially cut costs.

Participant L\_P1 discussed how the lack of structured federal regulations could cause companies to not be equal in basic guidelines, including the initial costs of projects. Evans, Burke, and Jarvik (2015) stated the FDA authority over medical device regulations had been called into question due to lax regulatory requirements. An example used by participant L\_P1 was the case of two companies, Company A and Company B. Company A decides to follow federal guidelines to enhance the IT security of medical device and software while Company B does not. If Company B manages to go several years without being caught, they will inevitably have more capital/cash on hand that can go into other expenditures. Company B will be more successful profit-wise than Company A because Company A went through the correct protocol. In the interim, Company B can later put their capital to use to invest in security. However, Company A, who was investing all along, had to go through the hardship and financial burden of this security investment, which decreased earnings. Participant L\_P1 believed that governed regulations should be met by all medical device companies. Based on company documents, in the scenario, if Company B were caught, fines would be imposed. Software developers need to know in advance the economic implication their security design choices add to the development process. Data breaches and negligent risk analysis for the chosen hardware and software led to a New York hospital being fined over four million dollars (McLeod and Dolezel, 2018). Participant I1\_P1 stated that federal laws changed a few years ago, making security updates required for all medical organizations.

Initially, companies that followed the security updates in a timely manner received incentives, while those who did not meet deadlines or upgrades were fined. Participant I2\_P3 iterated how not meeting federal requirements can cause the government agency to shut down the organization from producing new medical devices and software for a specified amount of time.

Sometimes medical device organizations will cut costs in product design due to outside factors, such as health insurance setting the price of medical device usage. Participant L\_P3 indicated that they designed feature enhancements for an MRI system, which did not produce much of a profit for the organization due to set fees given by insurance companies. Company documents for organization L referenced the unknowns of budgeting for unforeseen expenses that could affect the return on investments, which included the running cost of medical devices, and pricing from insurance companies. Company documents proposed gathering current rates and trends of similar medical devices/software. Participant L\_P1 further discussed how their organization loses money if an insurance company prices undercharge the proposed price, which was calculated to offset security and feature upgrades. Participant L\_P4 also emphasized that losing money leads to organizations removing features for the sake of making a profit. According to the *Managing Healthcare Technology Projects* document, even though stakeholders and developers provide the plan for the project, after analysis, it is the job of the financial officer to make choices to maintain the budget for the project.

### **Applications to Professional Practice**

This study explored strategies used by software developers to safeguard sensitive patient information collected, sent, and stored on medical devices swayed by external influences. Software developers should consider the external influences found in the SST theory when evaluating security and design strategies for medical software. The specific IT problem that formed from this research was that some software developers lack strategies to implement security measures to protect sensitive patient information collected, sent, and stored by medical devices. The research findings in this study revealed the strategies used by the participating organizations to enhance the security of medical devices. The study also included the advantages of analyzing the influences found in the SST theory as guidance for selecting specific design choices. Analyzing external factors that affect medical device software will help limit the vulnerabilities associated with technological advances of medical software. There were various perspectives on the best solution for selecting design choices to enhance security in medical devices. No aspects were terrible solutions, but it demonstrated that multiple influences should be examined in order to implement proper security measures.

Klonoff (2015) mentioned that if a security threat occurred, there could be an issue with the accuracy of information found on the device as well as issues completing the device designed tasks. If the device is hacked, sensitive personal information, such as social security number or healthcare-related information, could be leaked. Participants in this study indicated how security strategies are dependent on the software, hardware, and business needs of a project. Data collected from the participants and company documents

also indicated that external influences had an effect on medical device software and security due to the rapid changes in technology over the years. Without a one size fits all solution, the need to evaluate and analyze additional factors that are not internal to the medical device organization is prominent. Meticulous analysis allows software developers to choose between various security routes, which could potentially lead to different technological outcomes. Furthermore, it is vital and necessary for security design considerations to be handled during the initial analysis, throughout the development lifecycle, and continuing through the maintenance phase of the medical device/software.

During data analysis, I identified four primary themes: (1) securing medical device data, (2) social influences on medical device, (3) establishing standard policies for medical device security, and (4) factoring costs for medical device security. Both developers and stakeholders in medical organizations could use these themes as the underlying basis to aid in the analysis and selection of design choices. The knowledge from such information will enable software developers to ensure appropriate software designs and security choices are in place to decrease risks with sensitive patient data. When following the SST theory, software developers' attention shifts to the influences society has on technology instead of the impacts technology has on society. This framework will align with medical device security and aid in interpreting and understanding how hackers, technology advances, and patient/doctor usage of these devices for data transmission also influence the decisions of software developers.

Medical device organizations would benefit from having multiple teams to evaluate software being created. The first team should consist of subject matter experts (SMEs) who have proficiency with particular topics involving medical device software. The SMEs would be able to guide and debate on best actions for software design choices and security mechanisms. The second team would consist of security personnel whose responsibility is to search and handle security issues that may arise. Having a team in place to brainstorm possible scenarios that could interrupt the functionality of medical devices and create an incident response plan to handle these scenarios is crucial to software developers' security strategies (Zhou & Thai, 2016; Faiella et al., 2018). Zhou and Thai (2016) referred to a technique called the Failure Mode Effect Analysis (FMEA), used by security teams in various industries, to produce strategies in the event of software failures or attacks. These strategies can be incorporated into the security design of medical devices. Some participants pointed out that their organization had a similar document that gave insight on what to do next if security breaches or malfunctions occur. As stakeholders and software developers for medical device organizations, having teams and reference documents to enhance security measures would benefit the security of produced software.

### **Implications for Social Change**

This study explored how proper security strategies selection used by software developers can enhance the safety of sensitive patient information collected, sent, and stored on medical devices. To understand the strategic choices of stakeholders in medical device organizations, three organizations were involved in this study. Influences on

technological decisions extend far beyond medical device organizations and is a hidden driver behind most technological advances. This study reviewed the collaboration or lack thereof from software developers and SMEs to use diverse backgrounds, various levels of expertise, and varying perspectives and skillsets to select proper design strategies for medical device/software. The findings from this study will add to the existing body of knowledge by aiding in the understanding of typical security vulnerabilities, changes in federal and organizational regulations, economic factors, and how society influences the decisions of security design choices.

Medical device organizations may benefit from the strategies outlined in this study by utilizing some of the security strategies presented; these strategies aid in handling security challenges that are affected by the rapid technological changes in healthcare organizations. Data gathered in this study supported the conclusion that medical device organizations' security measures may be heightened if external factors are analyzed. This study may be of value to society as its findings may better influence software developers' decision to utilize new security strategies, which could lead to more secure medical applications for end-users. Data analysis indicated there is a relationship between influences found in the SST theory and software design choices used in medical device organizations. The influences of the SST were important as it relates to security design choices because the influences highlighted areas that are often overlooked such as social factors of unintentional threats or additional features that do not account for security changes. The research addressed characteristics for each factor found in the SST theory that may be worth adding to the analysis phase of medical device software design.

Using the SST theory, software developers will be able to identify how social, institutional, economic, and cultural factors may influence the direction of innovation, the practices used by software developers, and the outcomes of technological decisions based on external factors.

The study will also indirectly benefit users of the medical device/software, i.e., medical staff and patients. Major concerns for medical staff included the security and privacy of patient data while allowing the appropriate access to necessary medical staff. Key concerns for patients were the ease of use, costs, and security of medical devices/software. Medical devices play an essential role in patient healthcare by changing the way doctors and patients interact, and also creating a convenient way for patients to have immediate access to medical care. Medical device software security measures will always be a notable concern for medical device organizations due to the need to protect, prevent, mitigate, respond, and recover medical devices in the event of security threats. The knowledge learned from this study can aid in improving strategies selected for medical device security.

### **Recommendations for Action**

explored the strategies that software developers use to implement security measures to protect sensitive patient information on medical devices. Study findings determined that social, institutional, cultural, and economic factors affected decisions made regarding medical device security. Therefore, the themes in this study should be considered during the analysis phase for medical device software. Software developers



should design software with security as its core that incorporates external influences on the software.

For medical software organizations that do not use the team approach for analysis, using a team of SMEs would advance their design choices. The use of SMEs would be beneficial throughout the development life-cycle of the software by providing a wide variety of knowledge on particular technologies, processes, and techniques. The team should also confer potential threats and issues with the software from various points-of-views. An in-depth analysis that includes external influences for selected design strategies will most likely occur if external findings are mandatory to present with selected design strategies. Furthermore, designating a testing team to find and report vulnerabilities in the software would be an additional step to ensure the protection of the software through product release and maintenance of the software.

Results from this study are valuable to software developers, leaders, and stakeholders in medical device organizations. Indirectly, this study would be worthwhile to medical staff in providing a reliable tool for accurate diagnosis, improving patient-doctor communication, and providing quality remote patient monitoring. The results of this study will be distributed to the research participants via email. Additionally, results will be shared via scholarly and business journals.

### **Recommendations for Further Study**

One limitation of this study that was a concern was the well-rounded experience potential participants had throughout the life-cycle of medical device software creation. Initially, I was worried that software developers might not have insights on the various

external factors included in the SST theory in relation to design choices for medical software. Participants in this study were well-rounded due to their years of experience and added responsibilities while working for medical device organizations. However, I recommend adding additional participants from testing, management, leadership, sales perspectives, and so forth to provide more insight into external influences that affect design strategy selection. Another limitation was the location of the study participants; I recommend additional qualitative exploratory multiple case studies that include focus groups from medical device organizations from a larger region. Having a focus group to engage in medical device software issues and proposed solutions would provide unanticipated outcomes on medical device design choices.

The study findings also identified additional ways to evaluate medical device design choices. The study highlighted the significance of using a team during the initial analysis of projects but did not explore how to actually choose members for this team. Additionally, participants in the study acknowledged how organizational procedures were built on federal regulations for medical devices but did not explore the federal regulations or the organizations' culture in-depth. I recommend further research to explore building a team and the effects of organizational culture to mitigate risks with medical device data. One unexpected perception from a participant was the lack of mandated federal regulations for medical device organizations, which caused some organizations to evade following set procedures and also avoid being fined unless caught. Therefore, I recommend research on the loopholes of federal regulations in regards to medical device organizations.

## Reflections

Education-wise, my plan was to stop at my Masters. I told my mother that the only way I would continue was if I found a Doctorate's program online. Initially, when I started on this journey to obtaining a Doctorate, I was unaware of the rollercoaster ride I was in for. I thought the Doctorate program would be slightly more intense than receiving my Masters. With a second Master's degree to add to my accolades, I can say this journey has been a demanding yet rewarding process. Getting through the class portion of the Doctorate program was the easy part; the battle was staying focused and completing the dissertation. I did not think the dissertation portion would be easy, but I did not think I would have had as many setbacks. Even though I took close to a nine-month break before starting this journey again, I kept my eyes on the prize.

I chose to research medical device security due to my interest in portable medical devices to help those with disabilities. As a professional, I have worked as both a software developer and a QA analyst on many projects. However, none of the projects were in the medical field, and I was not involved in the security aspect or design strategies of these projects. Throughout the data analysis portion of this study, I did not have any bias that affected the results of the study. From the participants and research, I learned key strategies on thinking outside of the box and the need to understand a problem from as many varying perspectives during analysis and the design phases of projects that could help me as a professional.

### **Summary and Study Conclusions**

Healthcare providers choose to use medical devices in order to add to a patient's quality-of-life; however, since these devices must connect via computer networks, the threat of cybersecurity vulnerabilities is inevitable. Software developers use various strategies to implement security measures to protect sensitive patient information collected, sent, and stored on medical devices. There is not a one size fit all solution that will work for medical device security. Therefore, understanding that technology is partially society-driven is a necessary piece of the puzzle to create secure software/devices for use in medical organizations and with patients. This study supports the basis that there are external factors that affect medical device security based on the data collected from the three organizations in this study. As technology continues to grow, so will security threats, which is why having a solid foundation for analysis aids in limiting the risks of security vulnerabilities with medical devices. Although security will always be a concern in medical device organizations, enhancing the strategies for selecting security measures would allow software developers to ensure vulnerability decreases.

## References

- Aceto, G., Persico, V., & Pescape, A. (2018). The role of information and communication technologies in healthcare: Taxonomies, perspectives, and challenges. *Journal of Network and Computer Applications*, 107, 125-154.  
doi:10.1016/j.jnca.2018.02.008
- Ademe, B. W., Tebeje, B., & Molla, A. (2016). Availability and utilization of medical devices in Jimma zone hospitals, Southwest Ethiopia: A case study. *BMC Health Services Research*, 16(1), 287. doi:10.1186/s12913-016-1523-2.
- Agency for Healthcare and Quality. (2012, January). Coordinating care for adults with complex care needs in the patient-centered medical home: Challenges and solutions. Retrieved August 19, 2016, from <https://pcmh.ahrq.gov/>
- Al-Janabi, S., Al-Shourbaji, I., Shojafar, M., & Shamshirband, S. (2017). Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications. *Egyptian Informatics Journal*, 18(2), 113-122.  
doi:10.1016/j.eij.2016.11.001
- Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of things security: A survey. *Journal of Network and Computer Applications*, 88, 10-28.  
doi:10.1016/j.jnca.2017.04.002
- Ali, A., Shah, G. A., & Arshad, J. (2016). Energy efficient techniques for M2M communication: A survey. *Journal of Network and Computer Applications*, 68, 42-55. doi:10.3390/s19081830

- Allenby, C. E., Babiash, E. S., Blank, P. N., Carpenter, M. D., Lee, I. G., Li, R. B., . . . Gross, D. M. (2018). Analysis of the market, regulatory landscape, and current state of clinical trials pertaining to digital health. *Technology Transfer and Entrepreneurship*, 5(1), 21-34. doi:10.2174/2213809905666180816115016
- AlTawy, R., & Youssef, A. M. (2016). Security tradeoffs in cyber physical systems: A case study survey on implantable medical devices. *IEEE Access*, 4, 959-979. doi:10.1109/ACCESS.2016.2521727
- Anandarajan, M., & Malik, S. (2018). Protecting the internet of medical things: A situational crime-prevention approach. *Cogent Medicine*, 5(1), 1513349. doi:10.1080/2331205X.2018.1513349
- Auer, A., & Jarmai, K. (2018). Implementing responsible research and innovation practices in SMEs: Insights into drivers and barriers from the Austrian medical device sector. *Sustainability*, 10(1), 17. doi:10.3390/su10010017
- Azhar, R. A., Bochner, B., Catto, J., Goh, A. C., Kelly, J., Patel, H. D., . . . Desai, M. (2016). Enhanced recovery after urological surgery: A contemporary systematic review of outcomes, key elements, and research needs. *European Urology*, 70(1), 176-187. doi:10.1016/j.eururo.2016.02.051
- Baskerville, R. L., & Myers, M. D. (2015). Design ethnography in information systems. *Information Systems Journal*, 25(1), 23-46. doi:10.1111/isj.12055
- Bengtsson, M. (2016). How to plan and perform a qualitative study using content analysis. *NursingPlus Open*, 2, 8-14. doi:10.1016/j.npls.2016.01.001

- Bergh, D. D., Aguinis, H., Heavey, C., Ketchen, D. J., Boyd, B. K., Su, P., . . . Joo, H. (2016). Using meta-analytic structural equation modeling to advance strategic management research: Guidelines and an empirical illustration via the strategic leadership-performance relationship. *Strategic Management Journal*, *37*(3), 477-497. doi:10.1002/smj.2338
- Bertolini, A., Salvini, P., Pagliai, T., Morachioli, A., Acerbi, G., Cavallo, F., . . . Dario, P. (2016). On robots and insurance. *International Journal of Social Robotics*, *8*(3), 381-391. doi:10.1007/s12369-016-0360-0
- Bhanumathi, V., & Sangeetha, C. P. (2017). A guide for the selection of routing protocols in WBAN for healthcare applications. *Human-centric Computing and Information Sciences*, *7*(1), 1-19. doi:10.1186/s13673-017-0105-6
- Bianchi, M., Di Benedetto, A., Franzo, S., & Frattini, F. (2017). Selecting early adopters to foster the diffusion of innovations in industrial markets: Evidence from a multiple case study. *European Journal of Innovation Management*, *20*(4), 620-644. doi:10.1108/ejim-07-2016-006.
- Bidgoli, H. (2016). Integrating real life cases into a security system: Seven checklists for managers. *American Journal of Management*, *16*(4), 9-25. doi:10.33423/ajm.v16i4.1860
- Bijker, W. E., Hughes, T. P., Pinch, T., & Douglas, D. G. (2012). *The social construction of technological systems: New directions in the sociology and history of technology*. Cambridge, MA: MIT Press.

- Billingsley, L., & McKee, S. A. (2016). Cybersecurity in the clinical setting: Nurses' role in the expanding “internet of things”. *The Journal of Continuing Education in Nursing, 47*(8), 347-349. doi:10.3928/00220124-20160715-03
- Bilodeau, A., & Potvin, L. (2016). Unpacking complexity in public health interventions with the actor–network theory. *Health Promotion International, 33*(1), 173-181. doi:10.1093/heapro/daw062
- Birt, L., Scott, S., Cavers, D., Campbell, C., & Walter, F. (2016). Member checking: A tool to enhance trustworthiness or merely a nod to validation?. *Qualitative Health Research, 26*(13), 1802-1811. doi:10.1177/1049732316654870
- Blackwood, R. A., Maio, R. F., Mrdjenovich, A. J., Vandenbosch, T. M., Gordon, P. S., Shipman, E. L., & Hamilton, T. A. (2015). Analysis of the nature of IRB contingencies required for informed consent document approval. *Accountability in Research, 22*(4), 237-245. doi:10.1080/08989621.2014.956866
- Blake, L., Francis, V., Johnson, J., Khan, M., & McCray, T. (2017). Developing robust data management strategies for unprecedented challenges to healthcare information. *Journal of Leadership, Accountability and Ethics, 14*(1), 22-31. Retrieved from <http://www.na-businesspress.com/>
- Bolon, B., Baze, W., Shilling, C. J., Keatley, K. L., Patrick, D. J., & Schafer, K. A. (2018). Good laboratory practice in the academic setting: Fundamental principles for nonclinical safety assessment and GLP-compliant pathology support when developing innovative biomedical products. *ILAR Journal, 59*(1), 18-28. doi:10.1093/ilar/ily008.



- Booth, R. G., Andrusyszyn, M., Iwasiw, C., Donelle, L., & Compeau, D. (2016). Actor-network theory as a sociotechnical lens to explore the relationship of nurses and technology in practice: Methodological considerations for nursing research. *Nursing Inquiry*, 23(2), 109-120. doi:10.1111/nin.12118
- Borsci, S., Buckle, P., & Hanna, G. B. (2016). Why you need to include human factors in clinical and empirical studies of in vitro point of care devices? Review and future perspectives. *Expert Review of Medical Devices*, 13(4), 405-416. doi:10.1586/17434440.2016.1154277
- Brand, A. (2017). Medical device security: Patient safety and cost considerations. *Healthcare Financial Management*, 71(2), 28-31. Retrieved from <https://www.hfma.org/>
- Browning, J. G., & Tuma, S. (2015). If your heart skips a beat, it may have been hacked: Cybersecurity concerns with implanted medical devices. *South Carolina Law Review*, 67, 637-676. Retrieved from <https://heinonline.org/>
- Burns, A. J., Johnson, M. E., & Honeyman, P. (2016). A brief chronology of medical device security. *Communications of the ACM*, 59(10), 66-72. doi:10.1145/2890488
- Camara, C., Peris-Lopez, P., & Tapiador, J. E. (2015). Security and privacy issues in implantable medical devices: A comprehensive survey. *Journal of Biomedical Informatics*, 55, 272-289. doi:10.1016/j.jbi.2015.04.007

- Carter, N., Bryant-Lukosius, D., DiCenso, A., Blythe, J., & Neville, A. J. (2014, September). The use of triangulation in qualitative research. *Oncology Nursing Forum*, *41*(5), 545-547. doi:10.1188/14.ONF
- Castillo-Montoya, M. (2016). Preparing for interview research: The interview protocol refinement framework. *The Qualitative Report*, *21*(5), 811-831. Retrieved by <https://nsuworks.nova.edu/>.
- Cavusoglu, H., Cavusoglu, H., Son, J. Y., & Benbasat, I. (2015). Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources. *Information & Management*, *52*(4), 385-400. doi:10.1016/j.im.2014.12.004.
- Chan, H. K., Wang, X., Lacka, E., & Zhang, M. (2015). A mixed-method approach to extracting the value of social media data. *Production and Operations Management*, *25*(3), 568-583. doi:10.1111/poms.12390
- Chang, V., Kuo, Y. H., & Ramachandran, M. (2016). Cloud computing adoption framework: A security framework for business clouds. *Future Generation Computer Systems*, *57*, 24-41. doi:10.1016/j.future.2015.09.031
- Chao, H., Ho, C. Y., Leung, T. C., & Ng, T. (2017). To root or not to root? The economics of jailbreak. *Journal of Comparative Economics*, *45*(3), 481-497. doi:10.2139/ssrn.2274064
- Chen, Y. (2017). Design and implementation of wireless sensor cellular network based on android platform. *International Journal of Online Engineering*, *13*(5), 56-66. doi:10.3991/ijoe.v13i05.7048

- Chen, Y. J., Chiou, C. M., Huang, Y. W., Tu, P. W., Lee, Y. C., & Chien, C. H. (2018). A comparative study of medical device regulations: US, Europe, Canada, and Taiwan. *Therapeutic Innovation & Regulatory Science*, 52(1), 62-69. doi:10.1177/2168479017716712
- Chenail, R. J. (2009). Interviewing the investigator: Strategies for addressing instrumentation and researcher bias concerns in qualitative research. *Qualitative Report*, 13(4), 14-21. Retrieved from <https://nsuworks.nova.edu/>
- Christiansen, K., & Gasparin, M. (2016). Managing controversies in the fuzzy front end. *Creativity and Innovation Management*, 25(4), 500-514. doi:10.1111/caim.12174
- Cleary, M., Horsfall, J., & Hayter, M. (2014). Data collection and sampling in qualitative research: Does size matter? *Journal of Advanced Nursing*, 70(3), 473-475. doi:10.1111/jan.12163
- Coburn, J. C., & Grant, G. T. (2017). FDA regulatory pathways and technical considerations for the 3D printing of medical models and devices. In *3D printing in medicine* (pp. 97-111). Springer, Cham. doi:10.1007/978-3-319-61924-8\_10
- Coppola, R., & Morisio, M. (2016). Connected car: Technologies, issues, future trends. *ACM Computing Surveys (CSUR)*, 49(3), 1-36. doi:10.1145/2971482
- Cracchiolo, J. R., Roman, B. R., Kutler, D. I., Kuhel, W. I., & Cohen, M. A. (2016). Adoption of transoral robotic surgery compared with other surgical modalities for treatment of oropharyngeal squamous cell carcinoma. *Journal of Surgical Oncology*, 114(4), 405-411. doi:10.1002/jso.24353.

- Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2017). Organizational information security policies: A review and research framework. *European Journal of Information Systems*, 26(6), 605-641. doi:10.1057/s41303-017-0059-9
- Cronin, C. (2014). Using case study research as a rigorous form of inquiry. *Nurse Researcher*, 21(5), 19-27. doi:10.7748/nr.21.5.19.e1240
- Darwish, A., Hassanien, A. E., Elhoseny, M., Sangaiah, A. K., & Muhammad, K. (2019). The impact of the hybrid platform of internet of things and cloud computing on healthcare systems: Opportunities, challenges, and open problems. *Journal of Ambient Intelligence and Humanized Computing*, 10(10), 4151-4166. doi:10.1007/s12652-017-0659-1
- De Filippi, P. (2016). The interplay between decentralization and privacy: the case of blockchain technologies. *Journal of Peer Production*, 7, 1-19. Retrieved from <http://peerproduction.net/>
- Department of Health & Human Services. (n.d.). Health industry cybersecurity practices: Managing threats and protecting patients. Retrieved November 14, 2019, from <https://www.phe.gov/>
- Denscombe, M. (2014). *The good research guide: For small-scale social research projects*. New York, NY: McGraw-Hill Education.
- Diaz, M., Martín, C., & Rubio, B. (2016). State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing. *Journal of Network and Computer Applications*, 67, 99-117. doi:10.1016/j.jnca.2016.01.010

- Diaconu, K., Chen, Y. F., Cummins, C., Moyao, G. J., Manaseki-Holland, S., & Lilford, R. (2017). Methods for medical device and equipment procurement and prioritization within low-and middle-income countries: Findings of a systematic literature review. *Globalization and Health, 13*(1), 13-59. doi:10.1186/s12992-017-0280-2
- DiCicco-Bloom, B., & Crabtree, B. F. (2006). The qualitative research interview. *Medical Education, 40*(4), 314-321. doi:10.1111/j.1365-2929.2006.02418.x
- Dikko, M. (2016). Establishing construct validity and reliability: Pilot testing of a qualitative interview for research in Takaful (Islamic insurance). *Qualitative Report, 21*(3), 521-528. Retrieved from <https://nsuworks.nova.edu/>
- Dimitrov, D. V. (2016). Medical internet of things and big data in healthcare. *Healthcare Informatics Research, 22*(3), 156-163. doi:10.4258/hir.2016.22.3.156
- Doody, O., & Noonan, M. (2013). Preparing and conducting interviews to collect data. *Nurse Researcher, 20*(5), 28-32. doi:10.7748/nr2013.05.20.5.28.e327
- Doyle, P. A., Gurses, A. P., & Pronovost, P. J. (2017). Mastering medical devices for safe use. *American Journal of Medical Quality, 32*(1), 100-102. doi:10.1177/1062860616645857
- Dumay, J., & Rooney, J. (2016). Numbers versus narrative: An examination of a controversy. *Financial Accountability & Management, 32*(2), 202-231. doi:10.1111/faam.12086

- Effatparvar, M., Dehghan, M., & Rahmani, A. M. (2016). A comprehensive survey of energy-aware routing protocols in wireless body area sensor networks. *Journal of Medical Systems, 40*(9), 201. doi:10.1007/s10916-016-0556-8
- Elkatawneh, H. H. (2016). The five qualitative approaches: Problem, purpose, and questions/the role of theory in the five qualitative approaches/comparative case study. *SSRN Electronic Journal*, 1-18. doi:10.2139/ssrn.2761327
- Evans, B. J., Burke, W., & Jarvik, G. P. (2015). The FDA and genomic tests—getting regulation right. *New England Journal of Medicine, 372*(23), 2258-2264. doi:10.1056/NEJMsr1501194
- Faiella, G., Parand, A., Franklin, B. D., Chana, P., Cesarelli, M., Stanton, N. A., & Sevdalis, N. (2018). Expanding healthcare failure mode and effect analysis: A composite proactive risk analysis approach. *Reliability Engineering & System Safety, 169*, 117-126. doi:10.1016/j.ress.2017.08.003
- Farahani, B., Firouzi, F., Chang, V., Badaroglu, M., Constant, N., & Mankodiya, K. (2018). Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare. *Future Generation Computer Systems, 78*, 659-676. doi:10.1016/j.future.2017.04.036
- Farmer, T., Robinson, K., Elliott, S. J., & Eyles, J. (2006). Developing and implementing a triangulation protocol for qualitative health research. *Qualitative Health Research, 16*(3), 377-394. doi:10.1177/1049732305285708
- Federal Communications Commissions (FCC). (n.d.). Equipment authorization. Retrieved November 02, 2017, from <https://www.fcc.gov/>

- Fernandez-Aleman, J. L., Sánchez-Henarejos, A., Toval, A., Sanchez-García, A. B., Hernandez-Hernandez, I., & Fernandez-Luque, L. (2015). Analysis of health professional security behaviors in a real clinical setting: An empirical study. *International Journal of Medical Informatics*, *84*(6), 454-467. doi:10.1016/j.ijmedinf.2015.01.010
- Fitzgerald, S. K., Owens, C., Angles, M., Hockaday, D., Blackmore, M., & Ferguson, M. (2017). Reframing risk: A risk pathway method for identifying improvement through control and threat analysis. *Water Science and Technology: Water Supply*, *18*(1), 175-182. doi:10.2166/ws.2017.098
- Fusch, P. I., & Ness, L. R. (2015). Are we there yet? Data saturation in qualitative research. *Qualitative Report*, *20*(9), 1408-1416. Retrieved from <http://nsuworks.nova.edu/>
- Galvin, R. (2015). How many interviews are enough? Do qualitative interviews in building energy consumption research produce reliable knowledge? *Journal of Building Engineering*, *1*, 2-12. doi:10.1016/j.jobe.2014.12.001
- Genge, B., & Enachescu, C. (2015). ShoVAT: Shodan-based vulnerability assessment tool for internet-facing services. *Security and Communication Networks*, *9*(15), 2696-2714. doi:10.1002/sec.1262
- Ghamari, M., Janko, B., Sherratt, R. S., Harwin, W., Piechockic, R., & Soltanpur, C. (2016). A survey on wireless body area networks for ehealthcare systems in residential environments. *Sensors*, *16*(6), 831-864. doi:10.3390/s16060831

- Giger, J. T., Pope, N. D., Vogt, H. B., Gutierrez, C., Newland, L. A., Lemke, J., & Lawler, M. J. (2015). Remote patient monitoring acceptance trends among older adults residing in a frontier state. *Computers in Human Behavior, 44*, 174-182. doi:10.1016/j.chb.2014.11.044
- Gloyd, S., Wagenaar, B. H., Woelk, G. B., & Kalibala, S. (2016). Opportunities and challenges in conducting secondary analysis of HIV programmes using data from routine health information systems and personal health information. *Journal of the International AIDS Society, 19*(5), 1-6. doi:10.7448/ias.19.5.20847
- Gomes, B. D. T. P., Muniz, L. C. M., Silva e Silva, F. J., Ríos, L. E. T., & Endler, M. (2017). A comprehensive and scalable middleware for ambient assisted living based on cloud computing and internet of things. *Concurrency and Computation: Practice and Experience, 29*(11), 4043-4048. doi:10.1002/cpe.4043
- Gopalakrishna-Remani, V., Jones, R. P., & Camp, K. M. (2018). Levels of EMR adoption in US hospitals: An empirical examination of absorptive capacity, institutional pressures, top management beliefs, and participation. *Information Systems Frontiers, 1-20*. doi:10.1007/s10796-018-9836-9
- Graham, R., & Choi, K. S. (2016). Explaining African-American cell phone usage through the social shaping of technology approach. *Journal of African American Studies, 1*(20), 19-34. doi:10.1007/s12111-015-9317-x
- Grindrod, K., Boersema, J., Waked, K., Smith, V., Yang, J., & Gebotys, C. (2017). Locking it down: The privacy and security of mobile medication apps. *Canadian Pharmacists Journal, 150*(1), 60-66. doi:10.1177/1715163516680226



- Grossoehme, D. H. (2014). Overview of qualitative research. *Journal of Health Care Chaplaincy*, 20(3), 109-122. doi:10.1080/08854726.2014.925660
- Gustafsson, J. (2017). Single case studies vs. multiple case studies: A comparative study. Retrieved November 08, 2017, from [https:// www.diva-portal.org/](https://www.diva-portal.org/)
- Haghi, M., Thurow, K., & Stoll, R. (2017). Wearable devices in medical internet of things: Scientific research and commercially available devices. *Healthcare Informatics Research*, 23(1), 4-15. doi:10.4258/hir.2017.23.1.4
- Hall, J. L., & McGraw, D. (2014). For telehealth to succeed, privacy and security risks must be identified and addressed. *Health Affairs*, 33(2), 216-221. doi:10.1377/hlthaff.2013.0997
- Hatzivasilis, G., Papaefstathiou, I., & Manifavas, C. (2016). Software security, privacy, and dependability: Metrics and measurement. *IEEE Software*, 33(4), 46-54. doi:10.1109/ms.2016.61
- He, J., Baxter, S. L., Xu, J., Xu, J., Zhou, X., & Zhang, K. (2019). The practical implementation of artificial intelligence technologies in medicine. *Nature Medicine*, 25(1), 30-36. doi:10.1038/s41591-018-0307-0
- Hignett, S., Lang, A., Pickup, L., Ives, C., Fray, M., McKeown, C., . . . Bowie, P. (2016). More holes than cheese. What prevents the delivery of effective, high quality and safe health care in England?. *Ergonomics*, 1-10. doi:10.1080/00140139.2016.1245446
- Hogaboam, L., & Daim, T. (2018). Technology adoption potential of medical devices: The case of wearable sensor products for pervasive care in neurosurgery and

orthopedics. *Health Policy and Technology*, 7(4), 409-419.

doi:10.1016/j.hlpt.2018.10.011

Hoe, J., & Hoare, Z. (2013). Understanding quantitative research: Part 1. *Nursing Standard*, 27(15-17), 52-57. doi:10.7748/ns2012.12.27.15.52.c9485

Houghton, C., Casey, D., Shaw, D., & Murphy, K. (2013). Rigour in qualitative case-study research. *Nurse Researcher*, 20(4), 12-17.

doi:10.7748/nr2013.03.20.4.12.e326

Huddy, J. R., Ni, M., Mavroveli, S., Barlow, J., Williams, D., & Hanna, G. B. (2015). A research protocol for developing a point-of-care key evidence tool 'POCKET': A checklist for multidimensional evidence reporting on point-of-care in vitro diagnostics: Figure 1. *BMJ Open*, 5(7), 1-5. doi:10.1136/bmjopen-2015-007840

Hyett, N., Kenny, A., & Dickson-Swift, V. (2014). Methodology or method? A critical review of qualitative case study reports. *International Journal of Qualitative Studies on Health and Well-Being*, 9(1), 1-5. doi:10.3402/qhw.v9.23606

Imoniana, J. O., & Gartner, I. R. (2016). Critical remark on multi-criteria approach to corporate auditing risk assessment-evidence from Brazil. *International Journal of Auditing Technology*, 3(2), 128-149. doi:10.1504/ijaudit.2016.10002846

Johnson, M. L., Belin, J., Dorandeu, F., & Guille, M. (2017a). Strengthening the cost effectiveness of medical countermeasure development against rare biological threats: The Ebola outbreak. *Pharmaceutical Medicine*, 31(6), 423-436.

doi:10.1007/s40290-017-0211-9

- Johnson, M., O'Hara, R., Hirst, E., Weyman, A., Turner, J., Mason, S., . . . Siriwardena, A. N. (2017b). Multiple triangulation and collaborative research using qualitative methods to explore decision making in pre-hospital emergency care. *BMC Medical Research Methodology*, *17*(1), 1-11. doi:10.1186/s12874-017-0290-z
- Jung, Y., Kim, S., & Choi, B. (2016). Consumer valuation of the wearables: The case of smartwatches. *Computers in Human Behavior*, *63*, 899-905.  
doi:10.1016/j.chb.2016.06.040
- Kafle, V. P., Fukushima, Y., & Harai, H. (2016). Internet of things standardization in ITU and prospective networking technologies. *IEEE Communications Magazine*, *54*(9), 43-49. doi:10.1109/mcom.2016.7565271
- Kakucha, W., & Buya, I. (2018). Information system security mechanisms in financial management. *Journal of Information and Technology*, *2*(1), 1-16. Retrieved from <https://stratfordjournals.org/>
- Kallio, H., Pietila, A., Johnson, M., & Kangasniemi, M. (2016). Systematic methodological review: Developing a framework for a qualitative semi-structured interview guide. *Journal of Advanced Nursing*, *72*(12), 2954-2965.  
doi:10.1111/jan.13031
- Kamalodeen, V. J., & Jameson-Charles, M. (2016). A mixed methods research approach to exploring teacher participation in an online social networking website. *International Journal of Qualitative Methods*, *15*(1), 1-14.  
doi:10.1177/1609406915624578

- Kane, G. M., Bakker, C. A., & Balkenende, A. R. (2018). Towards design strategies for circular medical products. *Resources, Conservation and Recycling*, *135*, 38-47. doi:10.1016/j.resconrec.2017.07.030
- Kang, D., Jung, J., Lee, D., Kim, H., & Won, D. (2017). Security analysis and enhanced user authentication in proxy mobile IPv6 networks. *PloS One*, *12*(7), e0181031. doi:10.1371/journal.pone.0181031
- Karlsson, F., Kolkowska, E., & Prenkert, F. (2016). Inter-organisational information security: A systematic literature review. *Information and Computer Security*, *24*(5), 418-451. doi:10.1108/ics-11-2016-091
- Kartolo, A. B., & Kwantes, C. T. (2019). Organizational culture, perceived societal and organizational discrimination. *Equality, Diversity and Inclusion: An International Journal*, *38*(6), 602-618. doi:10.1108/EDI-10-2018-0191
- Kerkela, E. S., Jonsson, L., Lindwall, M., & Strand, J. (2015). Individual experiences following a 6-month exercise intervention: A qualitative study. *International Journal of Qualitative Studies on Health and Well-being*, *10*(1), 1-12. doi:10.3402/qhw.v10.26376
- Kerschner, C., & Ehlers, M. H. (2016). A framework of attitudes towards technology in theory and practice. *Ecological Economics*, *126*, 139-151. doi:10.1016/j.ecolecon.2016.02.010
- Khan, A. (2017). Virtual machine security. *International Journal of Information and Computer Security*, *9*(1/2), 49-84. doi:10.1504/ijics.2017.082839

- Khan, Y., Ostfeld, A. E., Lochner, C. M., Pierre, A., & Arias, A. C. (2016). Monitoring of vital signs with flexible and wearable medical devices. *Advanced Materials*, 28(22), 4373-4395. doi:10.1002/adma.201504366
- Kharel, J., Reda, H. T., & Shin, S. Y. (2019). Fog computing-based smart health monitoring system deploying lora wireless communication. *IETE Technical Review*, 36(1), 69-82. doi:10.1080/02564602.2017.1406828
- Khera, M. (2017). Think like a hacker. *Journal of Diabetes Science and Technology*, 11(2), 207-212. doi:10.1177/1932296816677576.
- Kikuchi, H. (2016). Social shaping of technological trajectories of Shinkansen. *Annals of Business Administrative Science*, 15(4), 175-186. doi:10.7880/abas.0160605a
- Klersy, C., Boriani, G., Silvestri, A. D., Mairesse, G. H., Braunschweig, F., Scotti, V., . . . Leyva, F. (2016). Effect of telemonitoring of cardiac implantable electronic devices on healthcare utilization: A meta-analysis of randomized controlled trials in patients with heart failure. *European Journal of Heart Failure*, 18(2), 195-204. doi:10.1002/ejhf.470
- Klonoff, D. C. (2015). Cybersecurity for connected diabetes devices. *Journal of Diabetes Science and Technology*, 9(5), 1143-1147. doi:10.1177/1932296815583334
- Kochhar, D., & Hilda, A. K. J. (2017). An approach for fault tolerance in cloud computing using machine learning technique. *International Journal of Pure and Applied Mathematics*, 117(22), 345-351. doi:10.13140/RG.2.2.31419.67366

- Kohnke, A., Sigler, K., & Shoemaker, D. (2016). Strategic risk management using the NIST risk management framework. *EDPACS*, 53(5), 1-6.  
doi:10.1080/07366981.2016.1160713
- Kraft, P., & Bausch, A. (2016). How do transformational leaders promote exploratory and exploitative innovation? Examining the black box through MASEM. *Journal of Product Innovation Management*, 33(6), 687-707. doi:10.1111/jpim.12335
- Kruse, C. S., Smith, B., Vanderlinden, H., & Nealand, A. (2017). Security techniques for the electronic health records. *Journal of Medical Systems*, 41(8), 127.  
doi:10.1007/s10916-017-0778-4
- Kumar, M., Kaur, N., Kaur, S., & Singh, R. (2016). Different security threats and its prevention in computer network. *International Journal of Advanced Research in Computer Science*, 7(6), 85-88. Retrieved from <https://www.researchgate.net/>
- Kumari, P., Mathew, L., & Syal, P. (2017). Increasing trend of wearables and multimodal interface for human activity monitoring: A review. *Biosensors and Bioelectronics*, 90, 298-307. doi:10.1016/j.bios.2016.12.001
- Lancaster, K. (2017). Confidentiality, anonymity and power relations in elite interviewing: Conducting qualitative policy research in a politicised domain. *International Journal of Social Research Methodology*, 20(1), 93-103.  
doi:10.1080/13645579.2015.1123555
- Latif, A. I., Othman, M., Suliman, A., & Daher, A. M. (2016). Current status, challenges and needs for pilgrim health record management sharing network, the case of Malaysia. *International Archives of Medicine*, 1-10. doi:10.3823/1883

- Lee, Y. (2014). Insight for writing a qualitative research paper. *Family and Consumer Sciences Research*, 43(1), 94-97. doi:10.1111/fcsr.12084
- Lee, K., Jung, S. Y., Hwang, H., Yoo, S., Baek, H. Y., Baek, R. M., & Kim, S. (2017). A novel concept for integrating and delivering health information using a comprehensive digital dashboard: An analysis of healthcare professionals' intention to adopt a new system and the trend of its real usage. *International Journal of Medical Informatics*, 97, 98-108. doi:10.1016/j.ijmedinf.2016.10.001
- Lee, M. S., & Soon, I. (2017). Taking a bite out of Apple: Jailbreaking and the confluence of brand loyalty, consumer resistance and the co-creation of value. *Journal of Product & Brand Management*, 26(4), 351-364. doi:10.1108/jpbm-11-2015-1045
- Lewis, R. B. (2004). NVivo 2.0 and ATLAS.ti 5.0: A comparative review of two popular qualitative data-analysis programs. *Field Methods*, 16(4), 439-464. doi:10.1177/1525822x04269174
- Lewis, S. (2015). Qualitative inquiry and research design: Choosing among five approaches. *Health Promotion Practice*, 16(4), 473-475. doi:10.1177/1524839915580941
- Li, S. (2014, June). A case study of interpretation learning strategies employed by successful interpretation learners. *TPLS Theory and Practice in Language Studies*, 4(6), 1303-1311. doi:10.4304/tpls.4.6.1303-1311

- Li, C., Wu, T., Chen, C., Lee, C., & Chen, C. (2017). An efficient user authentication and user anonymity scheme with provably security for IoT-based medical care system. *Sensors, 17*(7), 1482. doi:10.3390/s17071482
- Lin, Y. K., Lin, M., & Chen, H. (2019). Do electronic health records affect quality of care? Evidence from the HITECH Act. *Information Systems Research, 30*(1), 306-318. doi:10.1287/isre.2018.0813
- Lincoln, Y. S., & Tierney, W. G. (2004). Qualitative research and institutional review boards. *Qualitative Inquiry, 10*(2), 219-234. doi:10.1177/1077800403262361
- Losavio, M. M., Chow, K. P., Koltay, A., & James, J. (2018). The internet of things and the smart city: Legal challenges with digital forensics, privacy, and security. *Security and Privacy, 1*(3), e23. doi:10.1002/spy2.23
- Lu, T., Zhao, J., Zhao, L., Li, Y., & Zhang, X. (2015). Towards a framework for assuring cyber physical system security. *International Journal of Security and Its Applications, 9*(3), 25-40. doi:10.14257/ij sia.2015.9.3.04
- Mackay, H., & Gillespie, G. (1992). Extending the social shaping of technology approach: ideology and appropriation. *Social Studies of Science, 22*(4), 685-716. Retrieved from <https://jstor.org/>
- MacKenzie, D., & Wajcman, J. (1999). *The social shaping of technology* (2nd ed.). Maidenhead, United Kingdom: Open University Press.
- Madsen, H. M., Brown, R., Elle, M., & Mikkelsen, P. S. (2017). Social construction of stormwater control measures in Melbourne and Copenhagen: A discourse analysis of technological change, embedded meanings and potential mainstreaming.



*Technological Forecasting and Social Change*, 115, 198-209.

doi:10.1016/j.techfore.2016.10.003

Maheshwari, P. (2016). Security issues of cyber physical system: A review. *International Journal of Computer Applications*, 7-11. Retrieved from <https://www.ijcaonline.org/>

Mahmood, Z., Ning, H., Ullah, A., & Yao, X. (2017). Secure authentication and prescription safety protocol for telecare health services using ubiquitous IoT. *Applied Sciences*, 7(12), 1-22. doi:10.3390/app7101069

Malterud, K., Siersma, V. D., & Guassora, A. D. (2016). Sample size in qualitative interview studies. *Qualitative Health Research*, 26(13), 1753-1760. doi:10.1177/1049732315617444

Manohar, R. P., & Baburaj, E. (2016). Detection of stealthy denial of service (S-DoS) attacks in wireless sensor networks. *International Journal of Computer Science and Information Security*, 14(3), 343-346. doi:10.1049/iet-wss.2017.0029

Markley, J. D., Pakyz, A., Bernard, S., Lee, K., Appelbaum, N., Bearman, G., & Stevens, M. P. (2017). A survey to optimize the design of an antimicrobial stewardship smartphone app at an academic medical center. *American journal of Infection Control*, 45(3), 317-320. doi:10.1016/j.ajic.2016.09.026

Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. (2017). Cybersecurity and healthcare: How safe are we? *BMJ*, 1-4. doi:10.1136/bmj.j3179

- Martins, P. V., & Zacarias, M. (2017). An agile business process improvement methodology. *Procedia Computer Science*, *121*, 129-136.  
doi:10.1016/j.procs.2017.11.018
- Massis, A. D., & Kotlar, J. (2014). The case study method in family business research: Guidelines for qualitative scholarship. *Journal of Family Business Strategy*, *5*(1), 15-29. doi:10.1016/j.jfbs.2014.01.007
- Mathauer, I., & Imhoff, I. (2006). Health worker motivation in Africa: The role of non-financial incentives and human resource management tools. *Human Resources for Health*, *4*(1), 24-60. doi:10.1186/1478-4491-4-24
- Matko, A., & Takacs, T. (2017). Examination of the relationship between organizational culture and performance. *International Review of Applied Sciences and Engineering*, *8*(1), 99-105. doi:10.1556/1848.2017.8.1.14
- McCusker, K., & Gunaydin, S. (2015). Research using qualitative, quantitative or mixed methods and choice based on the research. *Perfusion*, *30*(7), 537-542.  
doi:10.1177/0267659114559116
- McDermid, F., Peters, K., Jackson, D., & Daly, J. (2014). Conducting qualitative research in the context of pre-existing peer and collegial relationships. *Nurse Researcher*, *21*(5), 28-33. doi:10.7748/nr.21.5.28.e1232
- Mcleod, A., & Dolezel, D. (2018). Cyber-analytics: Modeling factors associated with healthcare data breaches. *Decision Support Systems*, *108*, 57-68.  
doi:10.1016/j.dss.2018.02.007

- Mellit, A., Tina, G. M., & Kalogirou, S. A. (2018). Fault detection and diagnosis methods for photovoltaic systems: A review. *Renewable and Sustainable Energy Reviews*, *91*, 1-17. doi:10.1016/j.rser.2018.03.062
- Mikkonen, K., Elo, S., Kuivila, H., Tuomikoski, A., & Kaariainen, M. (2016). Culturally and linguistically diverse healthcare students' experiences of learning in a clinical environment: A systematic review of qualitative studies. *International Journal of Nursing Studies*, *54*, 173-187. doi:10.1016/j.ijnurstu.2015.06.004
- Mills, T. (2018). What has become of critique? Reassembling sociology after Latour. *British Journal of Sociology*, *69*(2), 286-305. doi:10.1111/1468-4446.12306
- Misra, S., Goswami, S., Taneja, C., & Mukherjee, A. (2016). Design and implementation analysis of a public key infrastructure-enabled security framework for ZigBee sensor networks. *International Journal of Communication Systems*, *29*(13), 1992-2014. Doi: 10.1002/dac.2893
- Moghaddasi, H., Sajjadi, S., & Kamkarhaghighi, M. (2016). Reasons in support of data security and data security management as two independent concepts: A new model. *Open Medical Informatics Journal*, *10*, 4-10.  
doi:10.2174/1874431101610010004
- Moore, W., & Frye, S. A. (2019). A review of the HIPAA, Part 1: History, PHI, and privacy and security rules. *Journal of Nuclear Medicine Technology*, jnmt-119. doi:10.2967/jnmt.119.227819.

- Morse, J. M. (2015). Critical analysis of strategies for determining rigor in qualitative inquiry. *Qualitative Health Research, 25*(9), 1212-1222.  
doi:10.1177/1049732315588501
- Nakrem, S., Solbjor, M., Pettersen, I. N., & Kleiven, H. H. (2018). Care relationships at stake? Home healthcare professionals' experiences with digital medicine dispensers – a qualitative study. *BMC Health Services Research, 18*(1), 26-36.  
doi:10.1186/s12913-018-2835-1
- National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. (1979). *The Belmont report: Ethical principles and guidelines for the protection of human subjects of research*. Washington, DC: U.S. Department of Health and Human Services.
- Nebeker, C., Lagare, T., Takemoto, M., Lewars, B., Crist, K., Bloss, C. S., & Kerr, J. (2016). Engaging research participants to inform the ethical conduct of mobile imaging, pervasive sensing, and location tracking research. *Translational Behavioral Medicine, 6*(4), 577-586. doi:10.1007/s13142-016-0426-4
- Ni, J., & Hu, J. (2017). Dynamics control of autonomous vehicle at driving limits and experiment on an autonomous formula racing car. *Mechanical Systems and Signal Processing, 90*, 154-174. doi:10.1016/j.ymssp.2016.12.017
- Niglas, K. (2007). Media review: Microsoft office excel spreadsheet software. *Journal of Mixed Methods Research, 1*(3), 297-299. doi:10.1177/1558689807301250
- Noble, D. F. (1984). *Forces of production: A social history of industrial automation* (p. 57). New Brunswick, NJ: Transaction Publishers.

- Noble, H., & Smith, J. (2015). Issues of validity and reliability in qualitative research. *Evidence-Based Nursing, 18*(2), 34-35. doi:10.1136/eb-2015-10205
- O'Cathain, A., Thomas, K. J., Drabble, S. J., Rudolph, A., & Hewison, J. (2013). What can qualitative research do for randomised controlled trials? A systematic mapping review. *BMJ Open, 3*(6), 1-15. doi:10.1136/bmjopen-2013-002889
- O'Riordan, C., & O'Connell, M. (2014). Predicting adult involvement in crime: Personality measures are significant, socio-economic measures are not. *Personality and Individual Differences, 68*, 98-101. doi:10.1016/j.paid.2014.04.010
- Oguz, F. (2016). Organizational influences in technology adoption decisions: A case study of digital libraries. *College & Research Libraries, 77*(3), 314-334. doi:10.5860/crl.77.3.314
- Orb, A., Eisenhauer, L., & Wynaden, D. (2001). Ethics in qualitative research. *Journal of Nursing Scholarship, 33*(1), 93-96. doi:10.1111/j.1547-5069.2001.00093.x
- Osborn, E., & Simpson, A. (2018). Risk and the small-scale cyber security decision making dialogue—a UK case study. *Computer Journal, 61*(4), 472-495. doi:10.1093/comjnl/bxx093
- Owen, G. T. (2014). Qualitative methods in higher education policy analysis: Using interviews and document analysis. *Qualitative Report, 19*(26), 1-19. Retrieved from <https://nsuworks.nova.edu/>
- Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful sampling for qualitative data collection and analysis in mixed

method implementation research. *Administration and Policy in Mental Health and Mental Health Services Research*, 42(5), 533-544. doi:10.1007/s10488-013-0528-y

Panwar, N., Sharma, S., & Singh, A. K. (2016). A survey on 5G: The next generation of mobile communication. *Physical Communication*, 18, 64-84.

doi:10.1016/j.phycom.2015.10.006

Papageorgiou, T., & Michaelides, P. G. (2016). Joseph Schumpeter and Thorstein Veblen on technological determinism, individualism and institutions. *European Journal of the History of Economic Thought*, 23(1), 1-30.

doi:10.1080/09672567.2013.792378

Pare, G., Leaver, C., & Bourget, C. (2018). Diffusion of the digital health self-tracking movement in Canada: Results of a national survey. *Journal of Medical Internet Research*, 20(5), e177. doi:10.2196/jmir.9388.

Perakslis, E. D., & Stanley, M. (2016). A cybersecurity primer for translational research. *Science Translational Medicine*, 8(322), 1-4. doi:10.1126/scitranslmed.aaa4493

Pesapane, F., Volonte, C., Codari, M., & Sardanelli, F. (2018). Artificial intelligence as a medical device in radiology: ethical and regulatory issues in Europe and the United States. *Insights into Imaging*, 9(5), 745-753. doi:10.1007/s13244-018-0645-y

Pitts, M. J., & Miller-Day, M. (2007). Upward turning points and positive rapport-development across time in researcher-participant relationships. *Qualitative Research*, 7(2), 177-201. doi:10.1177/1468794107071409

- Piwek, L., Ellis, D. A., Andrews, S., & Joinson, A. (2016). The rise of consumer health wearables: Promises and barriers. *PLoS Medicine*, *13*(2), 1-9.  
doi:10.1371/journal.pmed.1001953
- Podsakoff, P. M., MacKenzie, S. B., & Podsakoff, N. P. (2012). Sources of method bias in social science research and recommendations on how to control it. *Annual Review of Psychology*, *63*, 539-569. doi:10.1146/annurev-psych-120710-100452
- Polkinghorne, D. E. (2005). Language and meaning: Data collection in qualitative research. *Journal of Counseling Psychology*, *52*(2), 137-145. doi:10.1037/0022-0167.52.2.137
- Pronovost, P. J., Powers, J., & Jin, W. (2017). Technology development in health care is broken. *American Journal of Medical Quality*, *32*(2), 215-217.  
doi:10.1177/1062860616666165
- Pugnetti, C., & Schläpfer, R. (2018). Customer preferences and implicit tradeoffs in accident scenarios for self-driving vehicle algorithms. *Journal of Risk and Financial Management*, *11*(2), 28. doi:10.3390/jrfm11020028
- Qu, Y., Zheng, G., Wu, H., Ji, B., & Ma, H. (2019). An energy-efficient routing protocol for reliable data transmission in wireless body area networks. *Sensors*, *19*(19), 4238. doi:10.3390/s19194238
- Rajput, M., & Ghawte, U. (2017). Security challenges in wireless sensor networks. *International Journal of Computer Applications*, *168*(5), 24-28.  
doi:10.5120/ijca2017914414

Ranney, M. L., Meisel, Z. F., Choo, E. K., Garro, A. C., Sasson, C., & Guthrie, K. M.

(2015). Interview-based qualitative research in emergency care part II: Data collection, analysis and results reporting. *Academic Emergency Medicine*, 22(9), 1103-1112. doi:10.1111/acem.12735

Raza, U., Kulkarni, P., & Sooriyabandara, M. (2017). Low power wide area networks:

An overview. *IEEE Communications Surveys & Tutorials*, 19(2), 855-873. doi:10.1109/COMST.2017.2652320

Razzaq, M. A., Gill, S. H., Qureshi, M. A., & Ullah, S. (2017). Security issues in the

internet of things (IoT): A comprehensive study. *International Journal of Advanced Computer Science and Applications*, 8(6), 383. doi:10.14569/IJACSA.2017.080650

Rennkamp, B., & Bhuyan, R. (2016). The social shaping of nuclear energy technology in

South Africa. *Political Economy of Clean Energy Transitions*, 271-291. doi:10.1093/oso/9780198802242.003.0014

Roberts, P., Priest, H., & Traynor, M. (2006). Reliability and validity in research.

*Nursing Standard* (through 2013), 20(44), 41-45. doi:10.7748/ns2006.07.20.44.41.c6560

Robideaux, D. R., Robin, D. P., & Reidenbach, R. E. (2015). An examination of

demographic variables associated with ethical behaviors and perceptions of retailers. *Proceedings of the 1989 Academy of Marketing Science (AMS) Annual Conference Developments in Marketing Science: Proceedings of the Academy of Marketing Science*, 235-238. doi:10.1007/978-3-319-17055-8\_48



- Robinson, O. C. (2014). Sampling in interview-based qualitative research: A theoretical and practical guide. *Qualitative Research in Psychology, 11*(1), 25-41.  
doi:10.1080/14780887.2013.801543
- Robinson, J. C. (2015). Biomedical innovation in the era of health care spending constraints. *Health Affairs, 34*(2), 203-209. doi:10.1377/hlthaff.2014.0975
- Roman, R., Lopez, J., & Mambo, M. (2018). Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges. *Future Generation Computer Systems, 78*, 680-698. doi:10.1016/j.future.2016.11.009
- Ronquillo, J. G., & Zuckerman, D. M. (2017). Software-related recalls of health information technology and other medical devices: Implications for FDA regulation of digital health. *The Milbank Quarterly, 95*(3), 535-553.  
doi:10.1111/1468-0009.12278
- Rothrock, R. A., Kaplan, J., & Van Der Oord, F. (2018). The board's role in managing cybersecurity risks. *MIT Sloan Management Review, 59*(2), 12-15. Retrieved from <https://sloanreview.mit.edu/article>
- Ryan-Nicholls, K., & Will, C. (2009). Rigour in qualitative research: Mechanisms for control. *Nurse Researcher, 16*(3), 70-85. doi:10.7748/nr2009.04.16.3.70.c6947
- Sabi, H. M., Uzoka, F. M. E., Langmia, K., & Njeh, F. N. (2016). Conceptualizing a model for adoption of cloud computing in education. *International Journal of Information Management, 36*(2), 183-191. doi:10.1016/j.ijinfomgt.2015.11.010

- Sadoudi, L., Bocquet, M., Moulin, E., & Assaad, J. (2017). ZigBee sensor network platform for health monitoring of rails using ambient noise correlation. *Journal of Electrical Engineering*, 5, 143-150. doi:10.17265/2328-2223/2017.03.004
- Salesforce. (2017). A guide to sharing architecture. Retrieved November 2, 2019, from <https://resources.docs.salesforce.com/>
- Samaras, E. A., & Samaras, G. M. (2016). Confronting systemic challenges in interoperable medical device safety, security & usability. *Journal of Biomedical Informatics*, 63, 226-234. doi:10.1016/j.jbi.2016.08.024
- Sametingir, J., Rozenblit, J., Lysecky, R., & Ott, P. (2015). Security challenges for medical devices. *Communications of the ACM*, 58(4), 74-82. doi:10.1145/2667218
- San Cornelio, G., & Gomez Cruz, E. D. G. A. R. (2014). Co-creation and participation as a means of innovation in new media: An analysis of creativity in the photographic field. *International Journal of Communication*, 8, 1-20. Retrieved from <http://www.ijoc.org/>
- Sanjari, M., Bahramnezhad, F., Fomani, F. K., Shoghi, M., & Cheraghi, M. A. (2014). Ethical challenges of researchers in qualitative studies: The necessity to develop a specific guideline. *Journal of Medical Ethics and History of Medicine*, 7, 1-6. Retrieved from <http://jmehm.tums.ac.ir>
- Saunders, M. N. (2012). Choosing research participants. In *The practice of qualitative organizational research: Core methods and current challenges* (pp. 37-55). London, England: Sage Publications.

- Saunders, B., Kitzinger, J., & Kitzinger, C. (2015). Anonymising interview data: Challenges and compromise in practice. *Qualitative Research, 15*(5), 616-632. doi:10.1177/1468794114550439
- Saunders, B., Sim, J., Kingstone, T., Baker, S., Waterfield, J., Bartlam, B., . . . Jinks, C. (2017). Saturation in qualitative research: Exploring its conceptualization and operationalization. *Quality & Quantity, 1*-15. doi:10.1007/s11135-017-0574-8
- Seltzer, J. H., Heise, T., Carson, P., Canos, D., Hiatt, J. C., Vranckx, P., . . . Cutlip, D. E. (2017). Use of endpoint adjudication to improve the quality and validity of endpoint assessment for medical device development and post marketing evaluation: Rationale and best practices. A report from the cardiac safety research consortium. *American Heart Journal, 190*, 76-85. doi:10.1016/j.ahj.2017.05.009.
- Serban, M. A. (2016). Translational biomaterials-the journey from the bench to the market-think 'product'. *Current Opinion in Biotechnology, 40*, 31-34. doi:10.1016/j.copbio.2016.02.009
- Shahmarichatghieh, M., Harkonen, J., Haapasalo, H., & Tolonen, A. (2016). Product development activities over technology life-cycles in different generations. *International Journal of Product Lifecycle Management, 9*(1), 19-44. doi:10.1504/IJPLM.2016.078861
- Sherman, A. T., Delatte, D., Neary, M., Oliva, L., Phatak, D., Scheponik, T., . . . Thompson, J. (2017). Cybersecurity: Exploring core concepts through six scenarios. *Cryptologia, 1*-42. doi:10.1080/01611194.2017.1362063

- Simpson, A., & Quigley, C. F. (2016). Member checking process with adolescent students: Not just reading a transcript. *Qualitative Report, 21*(2), 377-392. Retrieved from <http://nsuworks.nova.edu/>
- Singh, U. K., Joshi, C., & Gaud, N. (2016). Measurement of security dangers in university network. *Measurement, 155*(1), 6-10. Retrieved from <https://www.ijcaonline.org/>
- Singh, A., Kumar, D., & Hotzel, J. (2018). IoT based information and communication system for enhancing underground mines safety and productivity: Genesis, taxonomy and open issues. *Ad Hoc Networks, 78*, 115-129. doi:10.1016/j.adhoc.2018.06.008
- Stamate, C., Magoulas, G. D., Küppers, S., Nomikou, E., Daskalopoulos, I., Jha, A., . . . Iannone, M. (2018). The cloudUPDRS app: a medical device for the clinical assessment of Parkinson's Disease. *Pervasive and Mobile Computing, 43*, 146-166. doi:10.1016/j.pmcj.2017.12.005
- Stetsenko, A. (2016). Moving beyond the relational worldview: Exploring the next steps premised on agency and a commitment to social change. *Human Development, 59*(5), 283-289. doi:10.1159/000452720
- Stine, I., Rice, M., Dunlap, S., & Pecarina, J. (2017). A cyber risk scoring system for medical devices. *International Journal of Critical Infrastructure Protection, 19*, 32-46. doi:10.1016/j.ijcip.2017.04.001

- Sung, Y., Sharma, P., Lopez, E., & Park, J. (2016). FS-OpenSecurity: A taxonomic modeling of security threats in SDN for future sustainable computing. *Sustainability*, 8(12), 919. doi:10.3390/su8090919
- Svensson, L., & Doumas, K. (2013). Contextual and analytic qualities of research methods exemplified in research on teaching. *Qualitative Inquiry*, 19(6), 441-450. doi:10.1177/1077800413482097
- Szabo, Z. (2017). The information security and IT security questions of pension payment. *Key Engineering Materials*, 755, 322-327. doi:10.4028/www.scientific.net/kem.755.322
- Talal, M., Zaidan, A. A., Zaidan, B. B., Albahri, A. S., Alamoodi, A. H., Albahri, O. S.,... & Mohammed, K. I. (2019). Smart home-based IoT for real-time and secure remote health monitoring of triage and priority system using body sensors: Multi-driven systematic review. *Journal of Medical Systems*, 43(3), 42. doi:10.1007/s10916-019-1158-z
- Talesh, S. A. (2018). Data breach, privacy, and cyber insurance: How insurance companies act as “compliance managers” for businesses. *Law & Social Inquiry*, 43(2), 417-440. doi:10.1111/lsi.12303
- Taylor, D., & Levin, M. (2014). Predicting mobile app usage for purchasing and information-sharing. *International Journal of Retail & Distribution Management*, 42(8), 759-774. doi:10.1108/ijrdm-11-2012-0108

- Terry, N. P., & Wiley, L. F. (2016). Liability for mobile health and wearable technologies. *Annals of Health Law.*, 25, 62. Retrieved from <https://papers.ssrn.com/>
- Tewari, A., & Verma, P. (2016). Security and privacy in E-healthcare monitoring with WBAN: A critical review. *International Journal of Computer Applications*, 136(11), 37-42. doi:10.5120/ijca2016908600
- The Departments and Agencies of the Federal Government. (2017, October). Electronic code of federal regulations. Retrieved November 02, 2017, from <https://www.ecfr.gov/>
- Thomas, D. R. (2017). Feedback from research participants: Are member checks useful in qualitative research? *Qualitative Research in Psychology*, 14(1), 23-41. doi:10.1080/14780887.2016.1219435
- Thompson, S. (2016). Worker cooperatives in the theory of the firm: Marx and Veblen on technological determinism. *Journal of Economic Issues*, 50(4), 913-939. doi:10.1080/00213624.2016.1249743
- Tibau, A., Bedard, P. L., Srikanthan, A., Ethier, J. L., Vera-Badillo, F. E., Templeton, A. J., ... & Amir, E. (2014). Author financial conflicts of interest, industry funding, and clinical practice guidelines for anticancer drugs. *Journal of Clinical Oncology*, 33(1), 100-106. doi:10.1200/jco.2014.57.8898
- Tomovic, S., Yoshigoe, K., Maljevic, I., & Radusinovic, I. (2017). Software-defined fog network architecture for IoT. *Wireless Personal Communications*, 92(1), 181-196. doi:10.1007/s11277-016-3845-0

- Tran, V., Porcher, R., Falissard, B., & Ravaud, P. (2016). Point of data saturation was assessed using resampling methods in a survey with open-ended questions. *Journal of Clinical Epidemiology*, 80, 88-96. doi:10.1016/j.jclinepi.2016.07.014
- Tsang, E. W. (2014). Case studies and generalization in information systems research: A critical realist perspective. *Journal of Strategic Information Systems*, 23(2), 174-186. doi:10.1016/j.jsis.2013.09.002
- U.S. Food and Drug Administration & Federal Communications Commissions. (2010, July 26). News & events (medical devices) - joint statement on wireless medical devices - U.S. Food and Drug Administration, Federal Communications Commission. Retrieved November 10, 2017, from <https://www.fda.gov/>
- U.S. Food and Drug Administration. (2015a, April 13). Cybersecurity of medical devices. Retrieved August 20, 2016, from <http://www.fda.gov/>
- U.S. Food and Drug Administration. (2015b, December 28). What is a medical device? Retrieved August 19, 2016, from <http://www.fda.gov/>
- U.S. Food and Drug Administration. (2015c, February 09). Mobile medical applications. Retrieved December 09, 2017, from <https://www.fda.gov/>
- U.S. Food and Drug Administration. (2017, October 10). Wireless medical devices. Retrieved November 02, 2017, from <https://www.fda.gov/>
- U.S. Food and Drug Administration. (2019, February). Principles of Premarket Pathways for Combination Products. Retrieved November 15, 2019, from <https://www.fda.gov/>

- Van Norman, G. A. (2016). Drugs and devices: Comparison of European and US approval processes. *JACC: Basic to Translational Science*, *1*(5), 399-412. doi:10.1016/j.jacbts.2016.06.003
- Vanniere, B., Guilyardi, E., Toniazzo, T., Madec, G., & Woolnough, S. (2014). A systematic approach to identify the sources of tropical SST errors in coupled models using the adjustment of initialised experiments. *Climate Dynamics*, *43*(7-8), 2261-2282. doi:10.1007/s00382-014-2051-6
- Varpio, L., Ajjawi, R., Monrouxe, L. V., O'Brien, B. C., & Rees, C. E. (2016). Shedding the cobra effect: Problematising thematic emergence, triangulation, saturation and member checking. *Medical Education*, *51*(1), 40-50. doi:10.1111/medu.13124
- Ventola, C. L. (2014). Mobile devices and apps for health care professionals: Uses and benefits. *Pharmacy and Therapeutics*, *39*(5), 356. Retrieved from <https://www.ncbi.nlm.nih.gov/>
- Vithanwattana, N., Mapp, G., & George, C. (2017). Developing a comprehensive information security framework for mHealth: A detailed analysis. *Journal of Reliable Intelligent Environments*, *3*(1), 21-39. doi:10.1007/s40860-017-0038-x
- Wan, J., Tang, S., Shu, Z., Li, D., Wang, S., Imran, M., & Vasilakos, A. V. (2016). Software-defined industrial internet of things in the context of industry 4.0. *IEEE Sensors Journal*, *16*(20), 7373-7380. doi:10.1109/JSEN.2016.2565621
- Wang, Y., Kung, L., & Byrd, T. A. (2018). Big data analytics: Understanding its capabilities and potential benefits for healthcare organizations. *Technological Forecasting and Social Change*, *126*, 3-13. doi:10.1016/j.techfore.2015.12.019



- Wangen, G., Hallstensen, C., & Snekkenes, E. (2017). A framework for estimating information security risk assessment method completeness. *International Journal of Information Security*, *16*(3), 1-19. doi:10.1007/s10207-017-0382-0
- Wei, Y., Wu, W., & Chu, Y. (2017). Performance evaluation of the recommendation mechanism of information security risk identification. *Neurocomputing*, *279*, 48-53. doi:10.1016/j.neucom.2017.05.106
- Weininger, S., Jaffe, M. B., & Goldman, J. M. (2017). The need to apply medical device informatics in developing standards for safe interoperable medical systems. *Anesthesia & Analgesia*, *124*(1), 127-135. doi:10.1213/ane.0000000000001386
- Williams, P., & Woodward, A. (2015). Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. *Medical Devices: Evidence and Research*, *8*, 305. doi:10.2147/mdr.s50048
- Williams, R., & Edge, D. (1996). The social shaping of technology. *Research Policy*, *25*(6), 865-899. doi:10.1016/0048-7333(96)00885-2.
- Wohlin, C., & Aurum, A. (2015). Towards a decision-making structure for selecting a research design in empirical software engineering. *Empirical Software Engineering*, *20*(6), 1427-1455. doi:10.1007/s10664-014-9319-7
- Woods, B., Coravos, A., & Corman, J. D. (2019). The case for a hippocratic oath for connected medical devices. *Journal of Medical Internet Research*, *21*(3), e12568. doi:10.2196/12568

- Yang, T. H., Ku, C. Y., & Liu, M. N. (2016). An integrated system for information security management with the unified framework. *Journal of Risk Research*, 19(1), 21-41. doi:10.1080/13669877.2014.940593
- Yang, T. C., Lo, N. W., Liaw, H. T., & Wu, W. C. (2017). A secure smart card authentication and authorization framework using in multimedia cloud. *Multimedia Tools and Applications*, 76(9), 11715-11737. doi:10.1007/s11042-016-3506-z
- Yazan, B. (2015). Three approaches to case study methods in education: Yin, Merriam, and Stake. *Qualitative Report*, 20(1), 134-152. Retrieved from <https://nsuworks.nova.edu/>
- Zeadally, S., Isaac, J. T., & Baig, Z. (2016). Security attacks and solutions in electronic health (E-health) systems. *Journal of Medical Systems*, 40(12), 263. doi:10.1007/s10916-016-0597-z
- Zhang, J., Huett, K., & Gratch, J. (2018, February). Do I need an IRB?: Computer science education research and institutional review board (IRB). In *Proceedings of the 49th ACM Technical Symposium on Computer Science Education* (pp. 1083-1083). ACM.
- Zhang, Y., & Wildemuth, B. M. (2016). Qualitative analysis of content. *Applications of Social Research Methods to Questions in Information and Library Science*, 318, 1-12. Retrieved from <https://philpapers.org/>

Zhou, Q., & Thai, V. V. (2016). Fuzzy and grey theories in failure mode and effect analysis for tanker equipment failure prediction. *Safety Science*, 83, 74-79.

doi:10.1016/j.ssci.2015.11.013

Zohrabi, M. (2013). Mixed method research: Instruments, validity, reliability and reporting findings. *Theory and Practice in Language Studies*, 3(2), 254-262.

doi:10.4304/tpls.3.2.254-262

## Appendix A: Human Research Participants Certificate of Completion



## Appendix B: Interview Protocol

**Interview Title:** Strategies to Lower Security Risks Involving Medical Devices in Patient Care

- A. I will introduce myself and thank the participant for agreeing to the interview.
- B. I will make sure that the consent form is signed and reiterate that participation is optional, and the participant can withdraw at anytime.
- C. I will give a brief overview of the purpose of this interview and ask the participant if he or she have any questions.
- D. I will inform the participant that the interview will be recorded and that I will be addressing them by their code name for the purpose of keeping the participant's identity confidential.
- E. I will start recording the conversation, announcing the interviewee by their associated code name, and also state the date and time.
- F. I will start the interview by asking the following questions:

### **Demographic Questions**

1. What is your primary role in the organization in regards to medical devices?
2. How long have you been working with the software for medical devices?
3. What are issues that occur when creating/updating software for medical devices?  
How are those issues mitigated?
4. How is medical device security handled in your organization?
5. How knowledgeable are you with the interrelation of cloud security and medical devices?


6. Is there a team that focuses directly on the security aspect of medical devices? If so, what is their role?
7. What are the different types of medical devices software created in your organization?




### **Interview Questions**

1. What are design choices used for creating the software for these medical devices?
  2. How do security policies in your organization and/or outside federal regulations affect how the software for medical devices is created?
  3. How do users and hackers affect how the software for medical devices is created (i.e., prevent jailbreaking)?
  4. Do budgets for healthcare data security affect security choices for medical devices?
  5. Are there any social influences (i.e., user acceptance) that affect how the software is developed?
  6. With technology always changing, what strategies do software developers in your organization use to keep the software in older medical devices compatible with new security measures?
  7. Is there any additional information you can provide on how medical device security strategies are influenced by internal or external influences?
- G. I will let the participant know that I am ending the interview.
- H. I will inform the participant that member checking will occur to ensure accuracy and validity of answers.

- I. I will thank the participant for being a part of this study, and make sure the participant has my contact information for any follow-up questions or concerns.

## Appendix C: Permission to Use Figures



 KE-EN 


---

**Legal**

**Terms of Use**

Last updated: 24 April 2019

Deloitte.com is comprised of various individual global, country, regional, or practice specific websites. Any such individual website is designated after the word "Location:" in the **upper right hand corner** of the webpage that you are viewing at any point during your use of deloitte.com.

These Terms of Use apply to the specific global, country, regional, or practice specific website that you were viewing within deloitte.com before clicking on these Terms of Use. Such individual website is referred to in these Terms of Use as "**this Website.**"

**By using this Website, you are agreeing to these Terms of Use. If you do not agree to these Terms of Use, then you are not allowed to use this Website and should immediately terminate such usage.**

The "**Deloitte Network**" refers to Deloitte Touche Tohmatsu Limited ("DTTL"), the member firms of DTTL, and their related entities. Each individual global, country, regional, or practice specific website within deloitte.com (as designated in the upper right hand corner of the webpage) is provided by an individual entity within the Deloitte Network.

Deloitte East Africa, which is the DTTL member firm in Kenya, is the entity within the Deloitte Network that is providing this Website and is referred to in these Terms of Use as "**we**", "**us**", or "**our**". Although parts of these Terms of Use may reference other entities in the Deloitte Network, these Terms of Use are only between you and us and not with any of those other entities.

**Use of Content: Restrictions: Privacy Statement**

Unless otherwise indicated in the relevant content, and on the condition that you comply with all of your obligations under these Terms of Use, you are authorized to view, copy, print, and distribute (but not modify) the content on this Website; provided that (i) such use is for informational, noncommercial purposes only, and (ii) any copy of the content that you make must include the copyright notice or other attribution associated with the content.

You are not authorized to copy or use any software, proprietary processes, or technology embodied or described in this Website.



You will comply with all applicable laws in accessing and using this Website.

You acknowledge that we may use your personal information and data according to our Privacy Statement and Cookie Notice, which are incorporated herein by this reference. You hereby agree to the terms of our Privacy Statement and Cookie Notice, including any obligations imposed on you therein.

**Intellectual Property Rights; No use of Deloitte names or logos**

Unless otherwise indicated, the content on this Website is provided by us or another entity within the Deloitte Network.

This Website and its contents are protected by copyright, trademark, and other laws of the United States and/or foreign countries. We and our licensors reserve all rights not expressly granted in these Terms of Use.

"Deloitte", "Touche", "Tohmatsu", "Deloitte Touche Tohmatsu", "Deloitte & Touche", the Deloitte logo, and local language variants of the foregoing trademarks, and certain product names that appear on this Website (collectively, the "Deloitte Marks"), are trademarks or registered trademarks of entities within the Deloitte Network. Except as expressly provided in these Terms of Use or as expressly authorized in writing by the relevant trademark owner, you shall not use any Deloitte Marks either alone or in combination with other words or design elements, including in any press release, advertisement, or other promotional or marketing material or media, whether in written, oral, electronic, visual or any other form.

References to other parties' trademarks on this Website are for identification purposes only and do not indicate that such parties have approved this Website or any of its contents. These Terms of Use do not grant you any right to use the trademarks of other parties.

**Disclaimers and Limitations of Liability**

THIS WEBSITE (INCLUDING WITHOUT LIMITATION ANY CONTENT OR OTHER PART THEREOF) CONTAINS GENERAL INFORMATION ONLY, AND WE ARE NOT, BY MEANS OF THIS WEBSITE, RENDERING PROFESSIONAL ADVICE OR SERVICES. BEFORE MAKING ANY DECISION OR TAKING ANY ACTION THAT MIGHT AFFECT YOUR FINANCES OR BUSINESS, YOU SHOULD CONSULT A QUALIFIED PROFESSIONAL ADVISOR.

THIS WEBSITE IS PROVIDED AS IS, AND WE MAKE NO EXPRESS OR IMPLIED REPRESENTATIONS OR WARRANTIES REGARDING IT. WITHOUT LIMITING THE FOREGOING, WE DO NOT WARRANT THAT THIS WEBSITE WILL BE SECURE, ERROR-FREE, FREE FROM VIRUSES OR MALICIOUS CODE, OR WILL MEET ANY PARTICULAR CRITERIA OF PERFORMANCE OR QUALITY. WE EXPRESSLY DISCLAIM ALL IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF MERCHANTABILITY, TITLE, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, COMPATIBILITY, SECURITY, AND ACCURACY.

YOUR USE OF THIS WEBSITE IS AT YOUR OWN RISK AND YOU ASSUME FULL RESPONSIBILITY AND RISK OF LOSS RESULTING FROM YOUR USAGE, INCLUDING, WITHOUT LIMITATION, WITH RESPECT TO LOSS OF SERVICE OR DATA. WE WILL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR PUNITIVE DAMAGES OR ANY OTHER DAMAGES WHATSOEVER, WHETHER IN AN ACTION OF CONTRACT, STATUTE, TORT (INCLUDING, WITHOUT LIMITATION, NEGLIGENCE), OR OTHERWISE, RELATING TO OR ARISING OUT OF THE USE OF THIS WEBSITE, EVEN IF WE KNEW, OR SHOULD HAVE KNOWN, OF THE POSSIBILITY OF SUCH DAMAGES.

CERTAIN LINKS ON THIS WEBSITE MAY LEAD TO WEBSITES, RESOURCES OR TOOLS MAINTAINED BY THIRD PARTIES OVER WHOM WE HAVE NO CONTROL, INCLUDING, WITHOUT LIMITATION, THOSE MAINTAINED BY OTHER ENTITIES WITHIN THE DELOITTE NETWORK OR INDIVIDUAL PERSONNEL OF SUCH ENTITIES. WITHOUT LIMITING ANY OF THE FOREGOING, WE MAKE NO EXPRESS OR IMPLIED REPRESENTATIONS OR WARRANTIES WHATSOEVER REGARDING SUCH WEBSITES, RESOURCES AND TOOLS, AND LINKS TO ANY SUCH WEBSITES, RESOURCES AND TOOLS SHOULD NOT BE CONSTRUED

AS AN ENDORSEMENT OF THEM OR THEIR CONTENT BY US.

THE ABOVE DISCLAIMERS AND LIMITATIONS OF LIABILITY SHALL BE APPLICABLE NOT ONLY TO US BUT ALSO TO EACH OTHER ENTITY WITHIN THE DELOITTE NETWORK AND TO OUR AND THEIR RESPECTIVE PERSONNEL.

THE ABOVE DISCLAIMERS AND LIMITATIONS OF LIABILITY ARE APPLICABLE TO THE FULLEST EXTENT PERMITTED BY LAW, WHETHER IN CONTRACT, STATUTE, TORT (INCLUDING, WITHOUT LIMITATION, NEGLIGENCE) OR OTHERWISE.

**Additional Terms**

If any portion of these Terms of Use is invalid or unenforceable in any jurisdiction, then (i) in that jurisdiction it shall be re-construed to the maximum effect permitted by law in order to effect its intent as nearly as possible, and the remainder of these Terms of Use shall remain in full force and effect, and (ii) in every other jurisdiction, all of these Terms of Use shall remain in full force and effect.

We may revise these Terms of Use at any time in our sole discretion by posting such revised Terms of Use at the Terms of Use link (i.e., this webpage that you are currently viewing) or elsewhere in this Website. Such revisions shall be effective as to you upon posting, unless explicitly stated by us. It is your responsibility to be aware of any such revised Terms of Use by checking this webpage. Your continued use of this Website following changes to these Terms of Use constitutes your agreement to the revised Terms of Use.

1/28/2020

RightsLink Printable License

**SPRINGER NATURE LICENSE  
TERMS AND CONDITIONS**

Jan 28, 2020

---

This Agreement between Walden University -- Brittany Thigpen ("You") and Springer Nature ("Springer Nature") consists of your license details and the terms and conditions provided by Springer Nature and Copyright Clearance Center.

License Number	4302750621098
License date	Mar 05, 2018
Licensed Content Publisher	Springer Nature
Licensed Content Publication	Springer eBook
Licensed Content Title	Wireless Body Area Network and Ultra-Wideband Communication
Licensed Content Author	Kasun Maduranga Silva Thotahewa, Jean-Michel Redouté, Mehmet Rasit Yuce
Licensed Content Date	Jan 1, 2014
Type of Use	Thesis/Dissertation
Requestor type	academic/university or research institute
Format	print and electronic
Portion	figures/tables/illustrations
Number of figures/tables/illustrations	1

1/28/2020

RightsLink Printable License

Will you be translating?	no
Circulation/distribution	<501
Author of this Springer Nature content	no
Title	Strategies to Lower Security Risks Involving Medical Devices in Patient Care
Instructor name	Dr. Charlie Shao
Institution name	Walden University
Expected presentation date	Sep 2018
Portions	Fig. 1.2 Key components of a WBAN
Requestor Location	Walden University [REDACTED]
Billing Type	Invoice
Billing Address	Walden University [REDACTED] United States Attn: Brittany Thigpen
Total	0.00 USD